NUCLEAR ENERGY INSTITUTE

**Lynnette Hendricks**
DIRECTOR, LICENSING
NUCLEAR GENERATION

March 15, 2002

Attention: Document Control Center
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: Guideline on Licensing Digital Upgrades

Enclosed for Nuclear Regulatory Commission endorsement is the final *Guideline on Licensing Digital Upgrades* (NEI 01-01 / EPRI TR-102348, Revision 1). The original guidelines for licensing digital system upgrades (EPRI TR-102348) were issued in 1993 and endorsed by the NRC in Generic Letter 95-02. The enclosure reflects consideration of NRC comments on the previous draft that was provided in our July 24, 2001, letter and discussed in a public meeting on October 11, 2001.

We view the submittal of this document for NRC staff review and endorsement as a means of exchanging information that is intended to support generic regulatory improvements. Therefore we believe an exemption from any review fees is warranted based on the criteria in footnote 4 of 10 CFR 170.21.

If you have any questions, please contact me at 202-739-8109 or Fred Madden at 202-739-8114.

Sincerely,

Lynnette Hendricks

Lynnette Hendricks

FWM/

Enclosure

Y601

c: Mr. J.P. Bongarra, USNRC MS: OWFN 6D17
Mr. J.A. Calvo, USNRC MS: OWFN 9D4
Mr. M. Chiramal, USNRC MS: OWFN 11D19
Mr. E.C. Marinos, USNRC MS: OWFN 11D19
Ms. E.M. McKenna, USNRC MS: OWFN 11E8
Mr. R. Torok, EPRI
Mr. P.C. Wen, USNRC MS: OWFN 11F1

# Guideline on Licensing Digital Upgrades
# EPRI TR-102348 Revision 1
# NEI 01-01

## A Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule

1002833

Final Report, March 2002

Prepared by
A Joint Task Force of
The Nuclear Energy Institute

and

The Electric Power Research Institute

EPRI Project Manager
R. Torok

NEI Project Manager
F. Madden

EPRI • 3412 Hillview Avenue, Palo Alto, California 94304 • PO Box 10412, Palo Alto, California 94303 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com

ORGANIZATION(S) THAT PREPARED THIS DOCUMENT

**MPR Associates, Inc.**

## ORDERING INFORMATION

Requests for copies of this report should be directed to EPRI Orders and Conferences, 1355 Willow Way, Suite 278, Concord, CA 94520, (800) 313-3774, press 2 or internally x5379, (925) 609-9169, (925) 609-1310 (fax).

# CITATIONS

This report was prepared by

MPR Associates, Inc.
320 King Street
Alexandria, VA 22314

Principal Investigators
E. Claude
R. Fink
K. Paul

This report describes research sponsored by EPRI and the US Department of Energy and supported by the Nuclear Energy Institute (NEI).

The report is a corporate document that should be cited in the literature in the following manner:

*Guideline on Licensing Digital Upgrades: EPRI TR-102348, Revision 1, NEI 01-01: A Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule*, EPRI, Palo Alto, CA: 2002. 1002833.

# REPORT SUMMARY

To continue meeting safety and reliability requirements while controlling operating costs, operators of nuclear power plants must be able to replace and upgrade equipment in a cost-effective manner. Upgrades to plant equipment and especially instrumentation and control (I&C) systems typically involve either replacement of analog devices with more modern digital technology or updating existing digital equipment. However, the use of digital technology has raised new design and licensing issues. This guide will help nuclear plant operators design, license and implement digital upgrades in a consistent, comprehensive manner.

## Background

Preferred upgrade solutions typically apply digital technology due to its ready availability, operational flexibility, and potential for performance and reliability improvements. Widespread implementation of digital upgrades has been hindered, however, by uncertainty regarding licensing, including the question of whether digital technology introduces new issues that require prior NRC approval. EPRI originally issued this guideline in 1993 to define a consensus approach that would resolve unsettled issues and help stabilize the treatment of the new technology for both licensees and regulators. A key issue was how to apply the 10 CFR 50.59 rule, which defines the criteria that establish when a license amendment is required before implementing plant changes. The NRC endorsed the original EPRI guideline in Generic Letter 95-02. Two important changes that affect the regulatory environment for digital upgrades have led to the need for this revision. First, much more guidance on ensuring high dependability with digital systems is now available. Key guides and standards have been reviewed and endorsed by the NRC, and the Standard Review Plan (NUREG-0800) has been expanded to cover digital systems. Second, the 10 CFR 50.59 rule was revised in 2000 and now allows changes that have minimal safety impact to be made without prior NRC review. The new rule uses criteria that can be difficult to apply to software-based systems and for which there is minimal precedent. For example, there is no consensus method for determining the likelihood of malfunction of software. The industry needed to update the 1993 guideline to address such issues and to help maintain a stable and standardized treatment of digital upgrades, while ensuring safety and reliability.

## Objective

To help nuclear plant operators implement and license digital upgrades in a consistent, comprehensive, and predictable manner.

## Approach

A task force of utility and industry representatives sponsored by EPRI and supported by the Nuclear Energy Institute (NEI) developed a guideline to help plant operators implement and license digital upgrades. The task force treated digital issues within the framework of the updated

10 CFR 50.59 regulation. Industry representatives and regulators reviewed drafts of the guideline. Their feedback reflected significant interest and expertise and helped strengthen the document.

## Results

This guide helps plant operators design and implement digital upgrades, perform 10 CFR 50.59 evaluations, and develop information to support licensing submittals. The approach in this document supplements NEI 96-07, Revision 1, *Guidelines for 10 CFR 50.59 Implementation.* The approach does not predetermine whether license amendments will be required for particular types of digital upgrades; this task remains the responsibility of the licensee. In essence, the guideline presents ways to address and resolve digital issues in the design and evaluation process. It suggests a failure analysis-based approach to manage risk that encompasses digital-specific issues and other possible failure causes, addressing both according to their potential effects at the system level. It also clarifies the treatment of potential software common cause failures and the use of defense-in-depth and diversity evaluations to confirm adequate backups exist where needed. Where possible, the guideline provides a road map to relevant standards and other sources of detailed guidance. While the guideline is designed primarily for digital upgrades to safety systems, it may also be applied to upgrades in non-safety systems.

## EPRI Perspective

This project is part of a multi-year EPRI initiative to help plant operators plan, implement, and license digital I&C upgrades in nuclear power plants. Other EPRI activities are providing specific methods and examples in areas such as software verification and validation, electromagnetic interference (EMI), and evaluation of commercial grade digital equipment for use in safety-related applications. This guideline is particularly significant in that it helps place the difficult issue of potential software common mode failure in the proper context, both in design and licensing.

Both the industry and the NRC staff have recognized the potential for enhanced safety and reliability that digital systems bring to the nuclear industry. However, uncertainties with the licensing treatment of issues related to digital technology have led several plant operators to postpone planned upgrades. With the great majority of plants now anticipating license renewal and decades of continued operation, the need to replace aging I&C systems has become more obvious and more acute. A consensus approach between regulators and licensees is therefore needed to ensure that the treatment of digital issues is predictable and consistent. It is anticipated that this guideline on licensing digital upgrades will receive endorsement and wide usage by the nuclear power industry.

## Keywords

Instrumentation and control
Digital upgrade
Licensing

# ABSTRACT

As existing instrumentation and control systems become obsolete, utilities are upgrading them with more modern systems based on digital technologies. This guideline is intended to assist utilities in implementing and licensing these digital upgrades. It includes guidance for carrying out the important steps in the design and implementation process to ensure that digital upgrade issues are adequately addressed, for performing the 10 CFR 50.59 evaluation and, if necessary, the License Amendment Request, and for complying with other regulatory requirements for digital equipment. This supplements the guidance contained in NEI 96-07, Revision 1, *Guidelines for 10 CFR 50.59 Implementation.*

The guide describes how the issues can be addressed within the upgrade design and evaluation process, specifically in the context of their potential effects on system functions and system-level failure modes. References are made to industry standards and other documents as appropriate. Additional guidance is provided in areas where existing standards or guidelines are not available, or where they need to be supplemented to adequately address the issues. The guide is intended primarily for digital upgrades to safety systems, but it also may be applied to upgrades in non-safety systems. The guidance can be applied to any modification that makes use of digital technology, whether small or large scale. This guideline supercedes EPRI TR-102348, *Guideline on Licensing Digital Upgrades*, 1993.

# ACKNOWLEDGMENTS

This guideline was prepared by a Digital Upgrade Licensing Task Force formed jointly by EPRI and NEI. The membership of the Task Force is shown below:

| | |
|---|---|
| Bruce Geddes, Co-chairman | Calvert Cliffs Nuclear Power Plant, Inc. |
| Bill Sotos, Co-chairman | STP Nuclear Operating Company |
| Marlan Albertson | AmerenUE |
| James Boatwright | TXU Electric |
| Eric Claude | MPR Associates, Inc. |
| Ray DiSandro | Exelon Nuclear |
| Larry Erin | Westinghouse |
| Bob Fink | MPR Associates, Inc. |
| Wayne Glidden | FirstEnergy Corporation |
| John Hefler | Altran Corporation |
| Lynnette Hendricks | Nuclear Energy Institute |
| Tim Hurst | Hurst Technologies, Corp. |
| Ron Jarrett | Tennessee Valley Authority |
| James Kilpatrick | Calvert Cliffs Nuclear Power Plant, Inc. |
| James McQuigan | Calvert Cliffs Nuclear Power Plant, Inc. |
| Fred Madden | Nuclear Energy Institute |
| Jerry Mauck | Framatome ANP |
| Wade Messer | Duke Energy |
| Joseph Naser | Electric Power Research Institute |
| Kristin Paul | MPR Associates, Inc. |
| Denny Popp | Westinghouse |
| Roy Raychaudhuri | Sargent and Lundy |
| Joe Ruether | Excel Energy |
| Clayton Scott | Invensys/Triconex |
| Bhupinder Singh | Jupiter Corporation |
| Rob Slough | TXU Electric |
| Jack Stringfellow | Southern Nuclear |
| Dinesh Taneja | Bechtel Power Corp. |
| Ray Torok | Electric Power Research Institute |

Also, the Task Force wished to acknowledge the contributions of many individuals in the industry and the Nuclear Regulatory Commission who reviewed and commented on drafts of the guideline. The suggestions and comments they provided have been extremely helpful in developing a workable approach for licensing digital upgrades.

# CONTENTS

# LIST OF FIGURES

# LIST OF TABLES

# 1 INTRODUCTION

## 1.1 Background

Nuclear utilities have a need to upgrade existing instrumentation and control (I&C) systems due to the growing problems of obsolescence, difficulty in obtaining replacement parts, and increased maintenance costs. There also is great incentive to take advantage of modern digital technologies which offer potential performance and reliability improvements. Widespread implementation of digital upgrades has been tempered, however, by uncertainty regarding licensing, including the question of whether digital technology introduces new issues that require prior Nuclear Regulatory Commission (NRC) approval.

EPRI originally issued this guideline in 1993 to address licensing questions and establish a well-defined, stable, and predictable regulatory framework within which digital system upgrades are accomplished in a safe and effective manner. This framework included methods to evaluate digital upgrades in the context of the 10 CFR 50.59 rule, which enables utilities to make certain changes to the plant without prior NRC review. The guideline also included a broad treatment of issues that are unique to digital equipment in relation to the 10 CFR 50.59 criteria. The original guideline was endorsed by the NRC in Generic Letter 95-02.

Since this guideline was first issued, two fundamental changes have taken place in the regulatory environment that affect licensing of digital upgrades. First, key guides and standards providing design requirements for digital-based systems have been reviewed and endorsed by the NRC. Regulatory review guidance in the Standard Review Plan (NUREG-0800) has also been expanded to cover digital systems. These guides and standards provide a broad base of common understanding for design, evaluation, and implementation of digital systems. Several industry initiatives and EPRI-sponsored projects have made use of these guides and standards to qualify digital equipment on a generic basis for safety related applications in nuclear power plants.

Second, 10 CFR 50.59 was revised in 2000 to better define the criteria that establish when prior NRC review (i.e., license amendment) is required before implementing plant changes. The revised rule allows changes that have minimal safety impact to be made without prior NRC review. Guidance in NEI 96-07, Revision 1, on implementing the revised rule further defines the "minimal impact" threshold, and focuses on the effects that plant changes have on design functions. These regulatory changes allow many digital upgrades to be made without the need for a license amendment.

Recognizing the impact of these changes on digital upgrades, EPRI convened a Task Force with support from the Nuclear Energy Institute (NEI) to update the original guidance contained in

EPRI TR-102348. The Task Force revised the original guideline to reflect the new 50.59 rule and complement NEI 96-07, Revision 1, with guidance for digital upgrade issues. Other changes were made to address key digital issues in the context of the engineering evaluations that are needed to support the 50.59 process.

Revisions to this guideline were made on the basis of the following underlying principles which also applied to the development of the original guideline:

- The existing licensing process, including 10 CFR 50.59, applies to digital upgrades. This document has been updated to reflect the revised 50.59 rule and the industry guidance for implementing this rule, NEI 96-07, Revision 1, "Guidelines for 10 CFR 50.59 Implementation." NEI 96-07, Revision 1 was endorsed by the NRC in Regulatory Guide 1.187.
- The issues associated with digital upgrades should be addressed in the context of their potential impact on the system being modified, reflecting the state of the system after the proposed upgrade is integrated with and installed in the plant. This helps to focus attention on the system functions that are important to the safe and reliable operation of the plant, and how these functions can be affected by potential failures of the digital equipment. In order to assess the potential for and impact of failures, a failure analysis with an appropriate level of detail is needed.
- Compliance with appropriate standards and guidelines is an important part of developing and installing high quality digital upgrades, and this guideline provides a road map to the relevant industry standards, guidelines, EPRI reports, and regulatory requirements.

## 1.2 Purpose of This Guideline

As described in the original guideline, this document is intended to assist utilities in implementing and licensing digital upgrades in a consistent and comprehensive manner. This includes guidance for:

- Carrying out important steps in the design and implementation process to ensure that digital upgrade issues are adequately addressed,
- Performing 10 CFR 50.59 evaluations for digital upgrades and, if necessary, preparing License Amendment Requests, and
- Complying with other regulatory requirements that pertain to digital equipment in nuclear power plants.

This document is intended primarily to address digital upgrades to safety systems. This guidance also may be applied to upgrades in non-safety systems at the discretion of the licensee. The guidance in this document applies to small- and large-scale digital upgrades – from the simple replacement of an individual analog meter with a microprocessor-based instrument, up to the complete change out of a reactor protection system with a new, integrated digital system. The guidance is not limited to instrumentation and control systems; it can also be applied to modifications or replacements of mechanical or electrical equipment if the new equipment makes use of digital technology (e.g., a new HVAC package that includes embedded microprocessors for control). This guideline also covers "digital-to-digital" changes; that is, changes to or replacement of digital-based systems.

## 1.3 Contents of This Guideline

Fundamental to the successful licensing of digital upgrades is proper handling of key technical issues during the design process. Of particular importance is a thorough understanding of the types of failures that could occur with digital equipment and the effects of these failures on the function of the system in which they are installed. This understanding ultimately guides both the design and licensing efforts. Therefore, the guideline first establishes the linkage between design and licensing activities, and then addresses the 10 CFR 50.59 issues in this context. The latter part of the guideline provides additional guidance on important elements of the design process and specific digital issues.

The contents of this guideline are structured to follow this approach in which the design process provides the answers needed for licensing:

- First, Section 2 provides definitions for key terms used in the guideline.
- Section 3 describes the design and implementation process for a plant modification and how the issues associated with digital upgrades are addressed in this process. The relevant concepts relating to failure analysis, handling of risks, and treatment of potential failures due to software are discussed in the context of the design process. Detailed guidance relating to failure analysis and the engineering evaluation issues that are unique to the design of digital systems is presented later in Section 5.
- Section 4 describes the licensing process for plant modifications that involve digital equipment. This includes guidance on evaluating potential changes to the plant Technical Specifications, performing 10 CFR 50.59 screening and evaluations, and navigating the license amendment process, if required. For 50.59 evaluations, guidance is provided to supplement NEI 96-07, Revision 1, on topics specific to digital upgrades.
- Section 5 provides more detailed guidance on the digital issues that are important both in the design of safe and reliable digital-based systems and in the engineering evaluations needed to support the 50.59 process. A variety of examples are included to illustrate failure analysis concepts and how the results are used in design and licensing.

# 2
# DEFINITIONS AND TERMINOLOGY

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

**Adverse effects.** Effects of a design change on a UFSAR-described design function that have the potential to increase the likelihood of malfunctions, increase consequences, create new accidents or otherwise meet the 10 CFR 50.59 evaluation criteria in paragraph 50.59(c)(2). [Excerpted from NEI 96-07, Revision 1]

**Basic component.** When applied to nuclear power plants licensed pursuant to 10 CFR Part 50, basic component means a structure, system, or component, or part thereof that affects its safety function, necessary to assure the integrity of the reactor coolant pressure boundary; the capability to shut down the reactor and maintain it in a safe shut down condition; or 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 50.34(a)(1) or 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 21.3]

**Change.** A modification or addition to, or removal from, the facility or procedures that affects a design function, method of performing or controlling the function, or an evaluation that the intended functions will be accomplished. [NEI 96-07, Revision 1]

**Commercial grade item (CGI).** When applied to nuclear power plants licensed pursuant to 10 CFR Part 50, commercial grade item (CGI) means a structure, system, or component, or part thereof that affects its safety function, that was not designed and manufactured as a basic component. Commercial grade items do not include items where the design and manufacturing process require in-process inspections and verifications to ensure that defects or failures to comply are identified and corrected (i.e., one or more critical characteristics of the item cannot be verified). [10 CFR 21.3]

**Commercial grade item dedication.** When applied to nuclear power plants licensed pursuant to 10 CFR Part 50, dedication is an acceptance process undertaken to provide reasonable assurance that a commercial grade item to be used as a basic component will perform its intended safety function and, in this respect, is deemed equivalent to an item designed and manufactured under a 10 CFR Part 50, Appendix B, quality assurance program. This assurance is achieved by identifying the critical characteristics of the item and verifying their acceptability by inspections, tests, or analyses performed by the purchaser or third-party dedicating entity after delivery, supplemented as necessary by one or more of the following: commercial grade surveys; product inspections or witness at hold points at the manufacturer's facility; and analysis of historical records for acceptable performance. In all cases, the dedication process is conducted in accordance with the applicable provisions of 10 CFR Part 50, Appendix B. The process is considered complete when the item is designated for use as a basic component. [10 CFR 21.3]

**Common cause failures**. Failures of equipment or systems that occur as a consequence of the same cause. The term is usually used with reference to redundant equipment or systems or to uses of identical equipment in multiple systems. Common cause failures can occur due to design, operational, environmental, or human factor initiators. Common cause failures in redundant systems compromise safety if the failures are *concurrent failures*, that is, failures which occur over a time interval during which it is not plausible that the failures would be corrected.

*Common mode failure*, by strict interpretation, has a meaning that is somewhat different from common cause failure because failure mode refers to the *manner* in which a component fails rather than the *cause* of the failure. However, because the discussions in this guideline are concerned with failures that can compromise safety and disable redundant systems or disable multiple systems using the same equipment, regardless of whether they are common mode or common cause, the two terms are used interchangeably in this document.

[Definitions adapted from the EPRI Equipment Qualification Reference Manual TR-100516 and ANSI/IEEE 352-1987]

**Computer**. Used broadly in this document to refer to any device which includes digital computer hardware, software (including firmware), and interfaces. [Derived from IEEE 7-4.3.2-1993] A microprocessor is considered as one 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]

**Consequences.** In 10 CFR 50.59, the term consequences refers to radiological doses, to either the public or the control room operators, as a result of any accident evaluated in the UFSAR, but does not apply to the occupational exposures resulting from routine operations, maintenance, testing, etc. [Excerpted from NEI 96-07, Revision 1]

**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]

**Defense-in-depth**. A concentric arrangement of protective barriers or means, all of which must be breached before a hazardous material or dangerous energy can adversely affect human beings or the environment. For instrumentation and control systems, the application of the defense in depth concept includes the control system; the reactor, trip, or scram system; the Engineered Safety Features Actuation System (ESFAS); the Anticipated Transients Without Scram (ATWS); and the monitoring and indicator system and operator actions based on existing plant procedures. The echelons may be considered to be concentrically arranged in that when the control system fails, the reactor trip system shuts down reactivity; when both the control system and the reactor trip system fail, the ESFAS continues to support the physical barriers to radiological release by cooling the fuel, thus allowing time for other measures to be taken by reactor operators to reduce reactivity. [NUREG/CR-6303]

**Dependability.** As used in this document, a broad concept incorporating various characteristics of digital equipment, including reliability, safety, availability, maintainability, and others. [EPRI TR-106439 (adapted from NUREG/CR-6294)]

**Design bases.** That information which identifies the specific functions to be performed by a structure, system, or component (SSC) of a facility, and the specific values or ranges of values chosen for controlling parameters as reference bounds for design. These values may be (1) restraints derived from generally accepted "state of the art" practices for achieving functional goals, or (2) requirements derived from analysis (based on calculation and/or experiments) of the effects of a postulated accident for which a structure, system, or component must meet its functional goals. [10 CFR 50.2]

**Design function.** UFSAR-described design bases functions and other SSC functions described in the UFSAR that support or impact design bases functions. Implicitly included within the meaning of design function are the conditions under which intended functions are required to be performed, such as equipment response times, process conditions, equipment qualification and single failure. [NEI 96-07, Revision 1]

Design bases functions are functions performed by systems, structures and components (SSCs) that are (1) required by, or otherwise necessary to comply with, regulations, license conditions, orders or technical specifications, or (2) credited in licensee safety analyses to meet NRC requirements. [NEI 96-07, Revision 1]

**Digital upgrade**. A modification to a plant system or component which involves installation of equipment containing one or more computers (see above definition of computer). These upgrades are often made to plant instrumentation and control (I&C) systems, but the term as used in this document also applies to the replacement of mechanical or electrical equipment when the new equipment contains a computer (e.g., installation of a new heating and ventilation system which includes controls that use one or more embedded microprocessors).

**Diversity**. The use of at least two different means for performing the same function. This can include diversity in *how* the function is performed (e.g., different algorithms, different variables sensed or physical principles applied, manual versus automatic) or in the *equipment* (different technologies, different hardware and/or software, different actuation means) used to perform the function. [Derived from IEC 880, the EPRI Equipment Qualification Reference Manual TR-100516, NUREG/CR-6303, and NUREG 800 Branch Technical Position (BTP)/HICB-19]

**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]

**Final Safety Analysis Report (FSAR).** The original FSAR is submitted with the application for the operating license and reviewed by the NRC in granting the initial license to operate the facility. The updated FSAR (UFSAR) is the original FSAR as periodically updated per the requirements of 10 CFR 50.71(e). The UFSAR describes the design bases, safety analyses, and facility operation under conditions of normal operation, anticipated operational occurrences, design basis accidents, external events, and natural phenomena for which the plant is designed to function.

The safety analyses described in the UFSAR demonstrate the integrity of the reactor coolant pressure boundary, the capability to shut down the reactor and maintain it in a safe shutdown condition, and the capability to prevent or mitigate the consequences of accidents.

[The above definition was adapted from NEI 98-03, Revision 1]

**Firmware**. Software that resides in read-only memory. [Adapted from IEEE 7-4.3.2-1993] An example is programmable read-only memory (PROM).

**Hardware**. Physical equipment used to process, store, or transmit computer programs or data. [ANSI/IEEE 610.12-1990]

**Human-system interface (HSI)**. All interfaces between the digital system and plant personnel including operators, maintenance technicians, and engineering personnel (e.g., display or control interfaces, test panels, configuration terminals, etc.). These interfaces include information and control resources used by plant personnel to perform their duties and tasks. Currently HSI is the term that is synonymous with and replacing human-machine interface (HMI) and man-machine interface (MMI). Principal HSIs are: alarms, information displays (including procedures), and controls. A HSI may be made up of hardware and software components and is characterized in terms of its important physical and functional characteristics.

**Malfunction.** In the context of 50.59, malfunction means the failure of a structure, system, or component to perform its intended design functions as described in the UFSAR (whether or not classified as safety-related in accordance with 10 CFR 50, Appendix B). [NEI 96-07, Revision 1]

**Microprocessor**. See computer.

**Radio-frequency interference (RFI)**. A form of electromagnetic interference (EMI). EMI is a broader definition which includes the entire electromagnetic spectrum, whereas RFI is more restricted to the radio-frequency band, generally considered to be between 10 kHz and 50 GHz. These terms (RFI and EMI) have been superseded by the broader term electromagnetic compatibility EMC.

**Redundancy**. The provision of alternative (identical or diverse) equipment or systems so that any one can perform the required function, regardless of the state of operation or failure of any other. [Derived from IEC 880]

**Reliability.** The characteristic of an item expressed by the probability that it will perform a required mission under stated conditions for a stated mission time. [IEEE-577-1991 and IEEE-352-1987]

**Safety related**. See safety related systems, structures, and components.

**Safety related systems, structures, and components (SSCs)**. Those systems, structures, and components that are relied upon to remain functional during and following design basis events to ensure (1) the integrity of the reactor coolant pressure boundary, (2) the capability to shut down the reactor and maintain it in a safe shutdown condition, or (3) the capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposures comparable to the applicable guideline exposures set forth in section 50.34 (a)(1) or section 100.11 of 10 CFR. [10 CFR 50.2]

**Screening.** The process used to determine whether a proposed change (for which 10 CFR 50.59 is applicable) requires a 10 CFR 50.59 evaluation to be performed. [NEI 96-07, Revision 1]

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

**Software safety analysis.** The process of identifying and analyzing potential hazards (which may result either from failures of the digital system or from external conditions or events) that can affect the safety of the system and the plant. The process focuses on identifying requirements that are needed in order to prevent or mitigate hazards. Regulatory review guidance in BTP/HICB-14 and in Regulatory Guide 1.173 states that there should be a defined safety analysis process in which responsibilities and activities are defined for each phase of the development process. Software safety analysis can be a part of the broader failure analysis, which is discussed in Section 5.

**System-level failure**. The failure of a system to perform its function, or a failure which affects the ability of another system to function. This phrase, used extensively in TR-102348, is enveloped by the broader phrase *results of a malfunction of an SSC*, which refers to the effect of the malfunction of an SSC in the Safety Analysis, as discussed in NEI 96-07, Revision 1.

**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]

# 3
# DIGITAL UPGRADE PROCESS

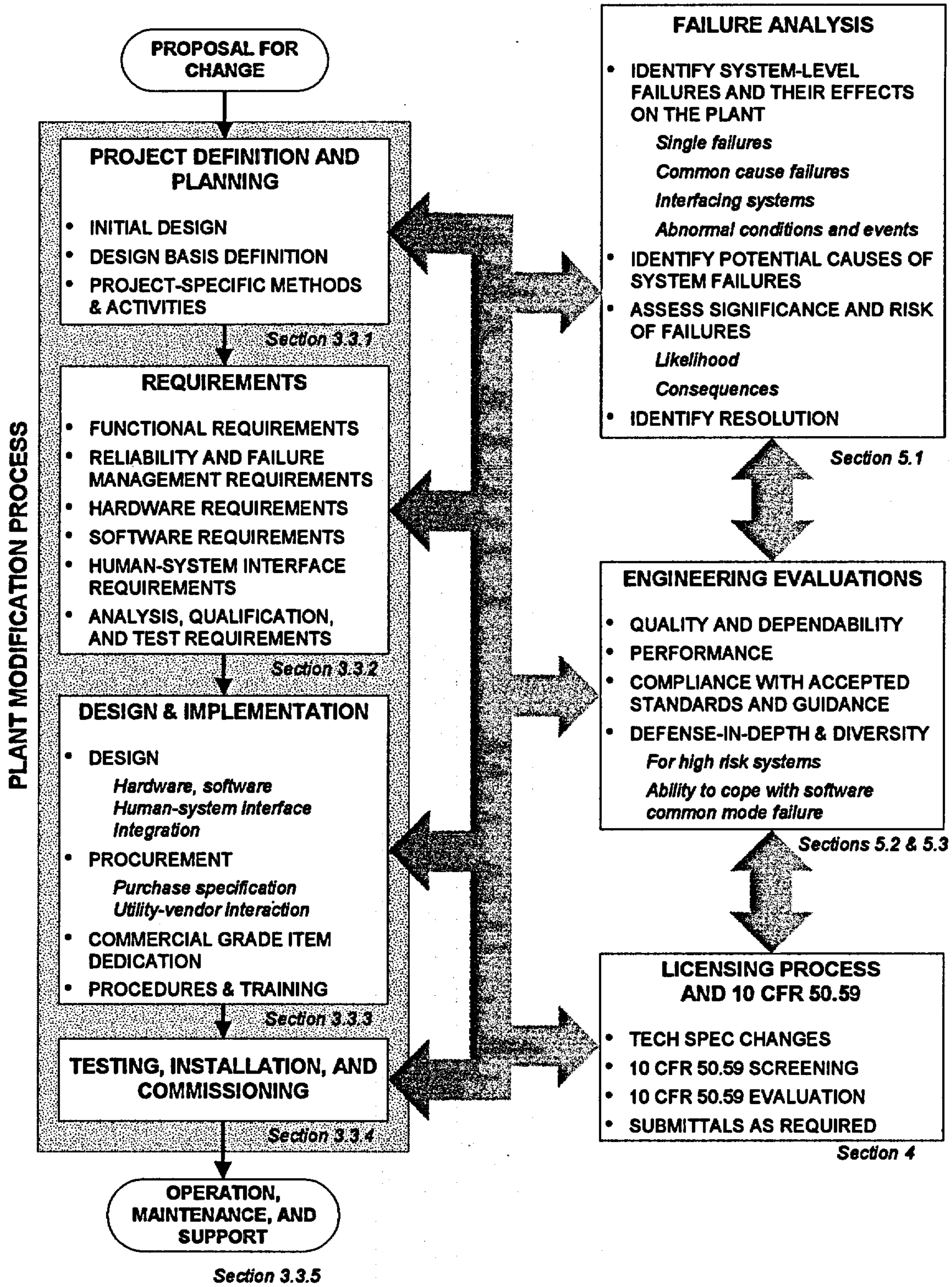
This section describes the process for design and implementation of plant upgrades and illustrates how the issues associated with licensing digital upgrades are addressed within this process. It is important that the design process thoroughly address the technical issues that affect digital upgrades, because the design solutions and supporting evaluations provide the bases needed to address the licensing issues. In addition, this section is intended to aid the user in identifying changes to plant processes that may be needed to support digital upgrades.

First, a general overview is given which describes the modification process. Next, the roles of failure analysis and other key engineering evaluations in design and licensing are discussed. Then, guidance is provided for some of the important steps in the plant modification process. The information presented here is intended to supplement more general guidance on the nuclear plant design change process, including NSAC-105, "Guidelines for Design and Procedure Changes in Nuclear Power Plants."

## 3.1 Digital Upgrade Process Overview

Figure 3-1 shows a typical digital upgrade design and implementation process. The main flow path down the left side of the figure shows the key steps in the modification process, starting with a change proposal and proceeding through installation, operation and maintenance. The process has been simplified for this figure. For example, the administrative and contractual steps involved in an upgrade project (e.g., forming the project team, selecting vendors, etc.) are not shown.

The upper right portion of the diagram shows activities associated with evaluation of potential system failures. In order to assess the impact of changes on plant design functions and safety, as well as on plant availability and investment protection, it is necessary to understand the potential failures (and other undesirable behaviors) of the system being modified and the effect that the modification will have on the likelihood and consequences of such failures. These activities will be referred to collectively as failure analysis in this guideline. This is not to imply, however, that there is necessarily a single analysis performed or technique applied, or that the results of these activities would necessarily be captured within a single document. Consideration of potential system failures should be an integral part of the design and implementation process for digital upgrades, interacting potentially with all of the key design, specification, and implementation activities, as shown on the diagram of Figure 3-1. Although it is singled out on the diagram for emphasis, failure analysis is not a stand-alone activity or one that operates outside the design process.




Note: Failure analysis and engineering evaluations are an integral part of the digital upgrade design process and are pulled out separately here for illustration purposes only.

**Figure 3-1**
**Digital Upgrade Process**

Engineering evaluations are shown in the middle of the right side of the diagram. Like failure analysis, engineering evaluations are activities that are performed as part of the design process, but are highlighted on Figure 3-1 for emphasis. Engineering evaluations include the collection of activities that are performed to demonstrate reasonable assurance that the system is safe and satisfies the specified requirements (e.g., for quality, dependability, and performance). This may include evaluating and interpreting the results of the failure analysis, design verifications, software V&V, and review of vendor software design and development processes. Where appropriate, analyses of overall defense-in-depth and diversity of the plant may be warranted to demonstrate the ability to cope with common cause failures.

Licensing activities are shown on the lower right side of the diagram, illustrating their interaction with the design and implementation activities. Section 4 discusses the licensing process in more detail and provides guidance for performing 10 CFR 50.59 evaluations for digital upgrades. Note that Figure 3-1 shows a tie between failure analysis, engineering evaluations, and licensing activities. This is important because many of the questions raised in licensing (e.g., 10 CFR 50.59 questions regarding likelihood and consequences of failures) can be resolved using information that comes out of the failure analysis and engineering evaluations.

## 3.2 Digital Issues in the Upgrade Process

Some of the key design issues for digital systems are addressed at a number of points in the process of specifying, designing, and implementing a digital upgrade. For example, software quality assurance processes require verification and validation activities to be carried out throughout the design, implementation, testing, installation, commissioning, and long-term maintenance of the upgrade. Similarly, human-system interface (HSI) design requirements need to be specified, appropriate verifications and validations performed, and necessary training, procedures, and administrative controls provided to enable adequate human performance and protect against human errors.

These issues all affect the potential for system failure. The issues are addressed specifically in the failure analysis (which interacts with all phases of the modification process), and it is in this context that ultimately they are resolved in the design.

### *3.2.1 Analyzing Failure and Risk in the Design Process*

Initially, failure analysis provides input in the form of design requirements such as requirements for features to preclude certain types of potential failures, or for failure detection and management within the system. As the design progresses and more details are available, additional potential failure modes may be identified, along with a need for corresponding resolutions which could affect the design. Section 5.1 of this guideline provides more detailed guidance for performing failure analyses.

Resolution of potential failures typically involves engineering judgment, with consideration of a number of factors. These factors include the likelihood of the failure, its importance based on system-level effects and the impact on the plant, the practicality of the options available for mitigating or eliminating the possibility of failure, the means of alerting the operator of the failure, and maintenance requirements to repair the failure. If the potential failure is judged to be significant, the resolution may be to add system design features that preclude or protect against the failure, take credit for backup from another system (defense-in-depth), or take actions that reduce the likelihood of the failure. If the problem is a lack of data to support an assessment of the likelihood of failure, the resolution may be to take action to develop the needed information (e.g., additional testing or verification activities to develop the needed confidence that the failure is adequately addressed).

Figure 3-2 illustrates how failure analysis is applied during the design process to understand and manage risk. Risk is a function of both the *likelihood* and the *consequences* of potential failures and hazards. Depending on the combination, risk could be judged to be negligible, non-negligible (but acceptable), or unacceptable. In practice, the design process identifies unacceptable risks and makes adjustments accordingly, so by the time a proposed change is ready for implementation in the plant or for NRC review, it will always lie in the region of negligible or acceptable risk.

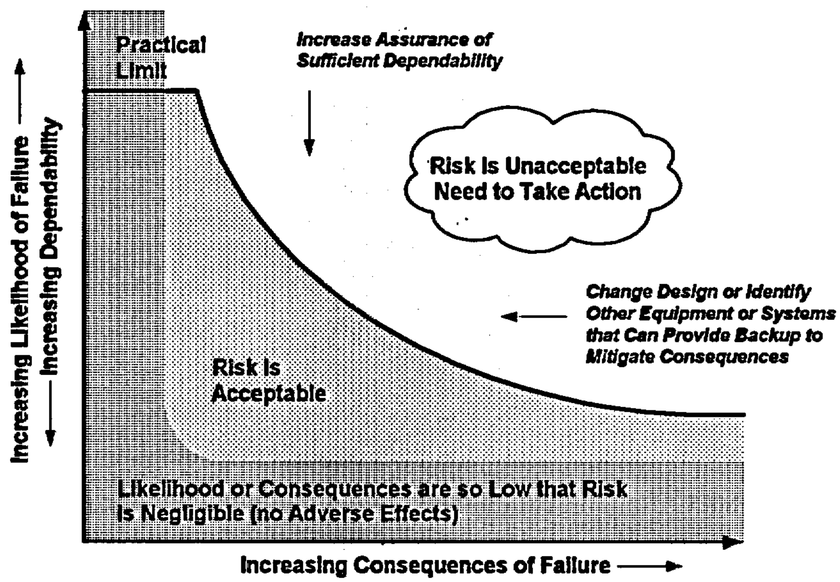



**Figure 3-2**
**Using Failure Analysis to Understand and Manage Risk**

At the engineering design stage, consequences could involve both safety and economic aspects although, for regulatory purposes, only the safety consequences are important. The likelihood of failure is based on a broad, usually qualitative, assessment of dependability that includes consideration of several factors including the software design process, hardware/software design, HSI design, fault tolerance, operating history, device complexity, system complexity, and testability. Plant Probabilistic Risk Assessment (PRA) data could also contribute to the assessment (See Example 5-3). These elements of dependability are discussed further in Section 5.3.

Note that Figure 3-2 is a general treatment of potential failure modes and hazards. It applies to any and all potential failures (including software common cause failure) and it applies regardless of whether the change under consideration affects an entire system or is only a component-level change.

### 3.2.2 Software Common Cause Failure

The safety model of a nuclear plant is based on an architecture of systems and equipment that uses a combination of multiple echelons of defense-in-depth and redundant equipment. This ensures that in the event of an accident or malfunction the plant can be brought to and maintained in a safe state. The plant is designed to cope with single active failures of hardware components in redundant safety systems, but common cause hardware failures (as a result of design deficiencies or manufacturing errors as discussed in IEEE 379) are considered beyond the design basis. The likelihood of hardware common cause failure is considered acceptably low due to factors such as the high quality standards applied in development and manufacture, physical separation of redundant equipment, and the recognition that degradation mechanisms that could result in common failures (e.g., corrosion or premature wear-out) are slow to develop and would be detected in maintenance and surveillance activities before they could disable a safety function.

Common cause failure vulnerability of digital safety I&C systems due to software errors could be considered as a special cause of single failure vulnerability, since the same software resides in the redundant channels of the system and a single undetected design error in the software could lead to a common cause failure of all redundant channels. For digital systems, the likelihood of software-related failure is minimized using the same basic approach of controlling the design, implementation, operation, and maintenance processes. Compliance with industry standards and regulatory requirements coupled with tests, evaluations, and reviews is used to assure a very low likelihood of failure. The important activities that are performed throughout the various phases of the digital upgrade process and that contribute to minimizing risk are summarized in Section 3.3 and discussed in detail in Section 5. Results of these activities are then used in the 10 CFR 50.59 process as described in Section 4. With respect to failures due to software, including common cause failures, the key to addressing these in licensing is having performed appropriate design, analysis and evaluation activities to provide reasonable assurance that such failures have a very low likelihood.

The conversion from analog to digital I&C systems often reduces the amount of discrete hardware involved in a system (e.g., replacing a large number of relays or analog electronic modules with a PLC), and thus reduces the risk of hardware common mode failures. However, most (but not all) digital I&C devices are significantly more complex than conventional analog devices when software is considered. As a result of this complexity, there can be a greater degree of uncertainty with respect to defining the likelihood of software-related failure of the device.

With this added degree of uncertainty regarding failures due to software, additional measures are appropriate for systems that are highly safety significant (i.e., high consequences on Figure 3-2) to achieve an acceptable level of risk. For digital upgrades to such systems, the defense-in-depth and diversity in the overall plant design are analyzed to assure that where there are vulnerabilities to common cause software failure, the plant has adequate capability to cope with these vulnerabilities (see Section 5.2). This defense-in-depth and diversity analysis is considered a beyond design basis concern, reflecting an understanding that while not quantifiable, the likelihood of a common cause software failure in a high quality digital system is significantly below that of a single active hardware failure. The analysis is performed as part of the design process, as the results could affect the design of the digital upgrade.

## 3.3 Phases of the Plant Modification Process

The phases of the plant modification process shown in Figure 3-1 are discussed below, along with specific guidance related to digital upgrades. EPRI 1001045, "Guideline on the Use of Pre-Qualified Digital Platforms for Safety and Non-Safety Applications in Nuclear Power Plants," provides more detailed guidance on important issues to consider in each of these phases.

This discussion pertains largely to the design and implementation of individual digital upgrades. The industry has recognized, however, that changes and enhancements in I&C system functionality that can accompany digital upgrades can have a significant impact on overall plant operation and maintenance and associated costs. To help assure successful implementation of individual upgrades and achieve long-term economic benefits, it is useful to develop an understanding of plant-wide I&C system needs and upgrade options, so that consistent criteria can be established, and regulatory, technical, and economic requirements can be met.

### *3.3.1 Project Definition and Planning*

- In terms of an individual upgrade, the types of activities to be performed and the methods and techniques to be applied should be identified early in the project, as they will affect licensing activities. Issues that should be considered include tools and techniques to specify requirements, failure analysis methodology and specific analysis techniques, software development methodology, tools and techniques for validation, levels of independence for verification, and skills and expertise needed on the project team.

The plant systems involved in the upgrade and their design and licensing bases should also be clearly defined early in the process. This includes defining:

- Objective(s) of the modification. What is the modification intended to accomplish? For example, is this a functionally equivalent replacement or is additional functionality to be provided as part of the modification? This can have a significant impact on 10 CFR 50.59 evaluations. Development of a conceptual design and functional requirements for the upgrade will assist in developing a clear statement of the objectives. Note that early evaluation of potential failure modes and their impact on the licensing evaluations can help ensure the objectives are appropriate from the beginning of the project.
- System(s) to be modified. What systems will be modified to support the objectives?
- Effects on other systems, training (including the simulator), and plant procedures. What are the effects from this modification on other systems? What interfaces are affected? What are the effects on the modified system of faults and potential failures from systems and components interfaced to the new system? This is important in determining the effects of potential failures in the upgraded equipment, and it can affect the 10 CFR 50.59 evaluations.

- Systems design basis and licensing basis. What are the design and licensing bases for the systems to be modified and for those that may be affected by the modification? System design documentation, design basis requirements, applicable sections of the UFSAR, Technical Specifications, and other design information should be used as appropriate.

### 3.3.2 Requirements

Experience in previous digital upgrades and lessons learned from software development have shown that proper specification of requirements is a key element in assuring adequate performance of the system. The increased flexibility and complexity of software-based systems makes specification of behaviors under unexpected, abnormal, and faulted conditions more complicated and more important than it would for analog systems. The user should specify both what the system must do and what it must not do. Section 2 of NSAC-105 provides general guidance on preparing design specifications for plant modifications. EPRI TR-108831 provides specific guidance on defining, analyzing, and tracking requirements for digital upgrades. EPRI 1001045 also provides guidance on defining plant-specific requirements for upgrades that involve pre-qualified digital platforms.

Most problems with digital systems occur in specifying the system, not in implementing the system or the software. The process should be very thorough in establishing the requirements for the upgraded system or equipment, identifying all interfaces and all the applicable design basis requirements. Also, the licensee should ensure that it adequately communicates to the vendor the plant-specific requirements and information needed to implement the design. It is important to continue communication between the vendor's design team and the licensee's system engineers, operators, maintenance, and testing staff to ensure that the system requirements have been correctly and completely included in the software and hardware design.

### 3.3.3 Design and Implementation

The goal of the design phase is to develop and document the detailed design of the digital system and the plant modification in accordance with the established requirements. Guidance on design issues for digital systems is provided in IEEE 7-4.3.2 and EPRI 1001045.

In this phase of the upgrade process, the final selection of the specific digital platform is made based on the requirements, hardware qualification tests are performed as necessary, commercial grade item dedication is performed as necessary, and application software is developed. It should be recognized that some of these choices might be implicit in the choice of vendor or third party integrator. As the detailed design is developed, the system failure analysis is expanded to address potential failures related to the specific digital platform, software tools, and application architecture to be used.

The licensee will also need to evaluate the quality and dependability of the digital system during this phase as input to the 10 CFR 50.59 process (see Section 4). Important elements to consider in such evaluations are discussed in Section 5.3.

### 3.3.4 Testing, Installation, and Commissioning

This step in the upgrade process includes activities such as factory acceptance tests, site acceptance tests, installation, and pre- and post-installation testing. System functionality and response to abnormal conditions and events should be tested to the maximum extent possible before installation in the plant, recognizing that while factory and simulator testing have limitations these activities are critical in verifying the adequacy of the design. Refer to IEEE 7-4.3.2 and EPRI 1001045 for additional guidance on these activities.

In many cases, acceptance tests can be performed with the digital upgrade installed in the plant simulator prior to installation in the plant. This allows the equipment to be tested with representative plant inputs and human-system interface verification and validation to be performed prior to installation. However, it is also necessary to maintain simulator fidelity with the actual plant configuration. Consequently, for large digital upgrades, a separate mock-up facility may be needed to allow testing and training on the new equipment before it is installed while still enabling operators to maintain their qualifications with the existing equipment.

### 3.3.5 Operation, Maintenance, and Support

The life cycle of a digital system continues even after it has been successfully installed in the plant. When the system is put into service, the licensee needs to be sure that sufficient and appropriate procedures are in place to monitor and evaluate error reports generated by the digital equipment vendor, maintain configuration control as the digital equipment is repaired, upgraded or modified, and ensure documentation is kept up to date. Maintaining configuration control is critical to assure that the licensing basis is preserved.

In terms of system operation, the need for procedures and training of personnel should be defined early in the upgrade process. Procedures should cover configuring, operating, maintaining, and modifying the upgraded equipment, including configuration control of hardware, software, and data (e.g., setpoints). Also, specific needs for training of operations, maintenance, and engineering personnel should be identified. The licensee should ensure that personnel will be fully informed, knowledgeable of the system and the important characteristics of the new equipment (e.g., its potential failure modes and how they differ from the previous equipment), and fully trained on the tasks they are expected to perform with the system and the associated procedures. Note that the impact of a digital upgrade on procedures and training can vary widely depending on the scope and complexity of the upgrade.

On-going maintenance may also need to include periodic testing (i.e., surveillance testing) such as that described in IEEE-338, "Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems," and Regulatory Guide 1.22, "Periodic Testing of Protection System Actuation Functions." Guidance on developing strategies for periodic testing of digital equipment is also discussed in EPRI 1001045 and BTP/HICB-17, "Guidance on Self-Test and Surveillance Test Provisions."

# 4
# LICENSING PROCESS AND 10 CFR 50.59

As part of making a change to a nuclear power plant, the licensee performs the necessary reviews and evaluations to ensure that the change is safe, verifies that the change meets the applicable regulations, determines the effect of the change on the plant's licensing basis, and determines whether approval of the change is needed from the NRC. The key regulation that governs changes to a licensed nuclear facility is 10 CFR 50.59. Guidance on implementing this regulation is provided in NEI 96-07, Revision 1, which has been endorsed by the NRC in Regulatory Guide 1.187.

Under the provisions of 10 CFR 50.59, the licensee is allowed to (a) make changes in the facility as described in the Updated Final Safety Analysis Report (UFSAR), (b) make changes to the procedures as described in the UFSAR, and (c) conduct tests or experiments not described in the UFSAR, without NRC review and approval prior to implementation, provided the proposed activity does not involve a change in the Technical Specifications and meets the criteria defined in 10 CFR 50.59.

The 10 CFR 50.59 process, shown in Figure 4-1, applies to digital upgrades as it does to other plant modifications. However, there are specific considerations that should be addressed including, for example, different potential failure modes of digital equipment as opposed to the equipment being replaced, the effect of combining functions of previously separate devices into one digital device, and the potential for software common cause failures. As previously discussed in Section 3, these digital considerations are addressed in the design process, including in failure analyses and other engineering evaluations. These evaluations are important inputs to the licensing process as shown in Figure 4-1.

It can be beneficial to inform the NRC early in the process, prior to determining what formal submittals may be required, about the intention to make a significant digital upgrade to a safety system. This can help avoid misunderstandings and facilitate useful and timely interactions between the licensee and NRC, potentially leading to a smoother licensing process for the upgrade. However, the project should be clearly defined (see Section 3.3.1) before extensive dialogue is initiated.

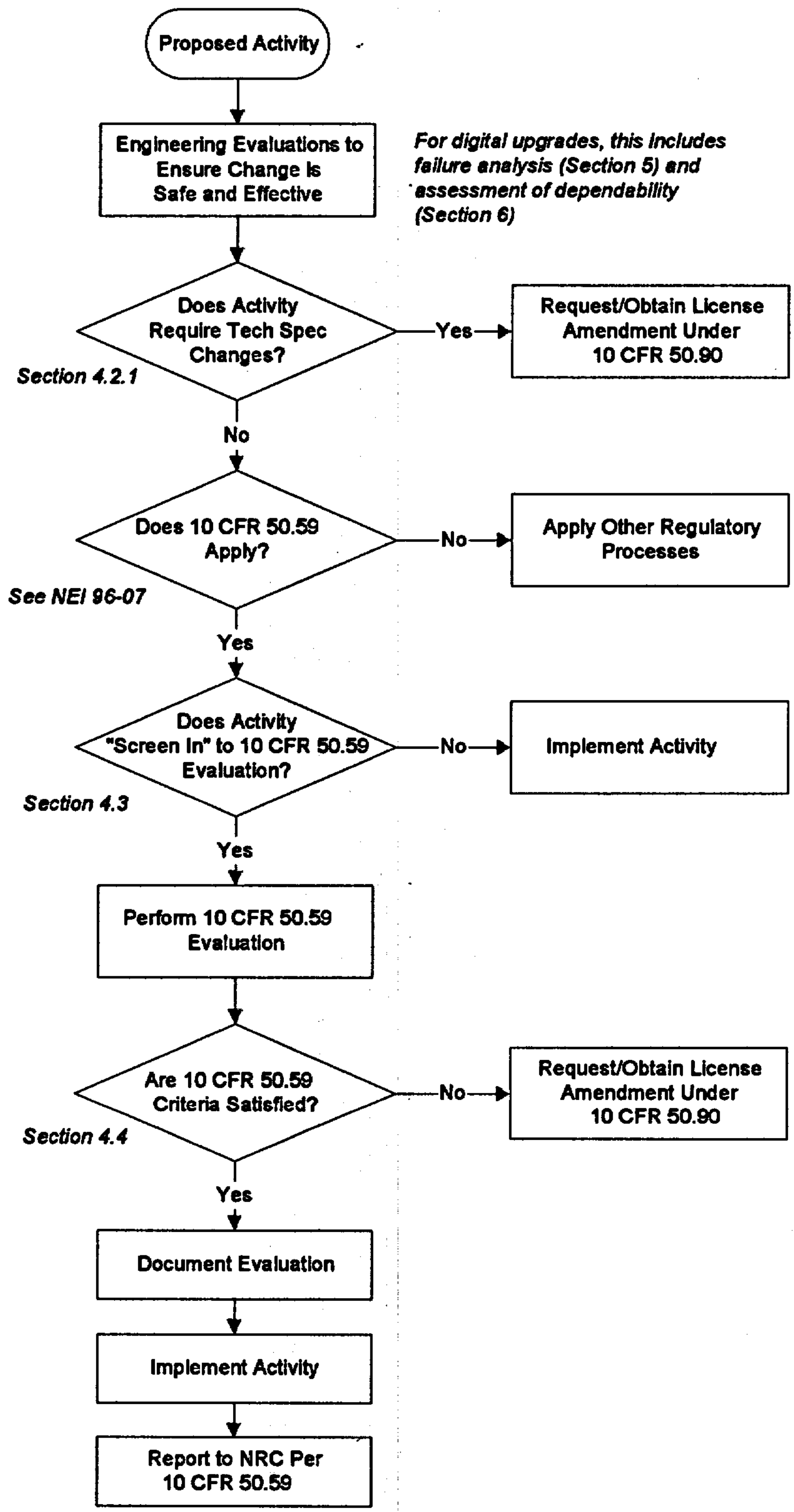



**Figure 4-1**
**10 CFR 50.59 Process (from NEI 96-07, Revision 1)**

## 4.1 Engineering Evaluations

For digital upgrades one of the challenges in the 10 CFR 50.59 process is addressing the effect of software, and potential failures due to software, on the design function. The answer lies in the engineering evaluations that are performed throughout the design process.

### *4.1.1 Use of Engineering Evaluations*

One of the key considerations in licensing digital upgrades is determining whether failures due to software are as likely as other potential failures addressed in the UFSAR. This issue is addressed by establishing reasonable assurance that such failures are unlikely, based on the engineering evaluations performed as part of the design process. As illustrated in Figure 4-2, two key elements of the engineering evaluations are evaluating the dependability of the digital equipment and its associated software considering the issues discussed in Section 5.3, and analyzing potential failures as discussed in Section 5.1.

Results of these engineering evaluations are then used as a basis for determining the risk of failures. As shown in Figure 3-2, if either the likelihood of failure or the consequences of failure are sufficiently low, then the risk is negligible.

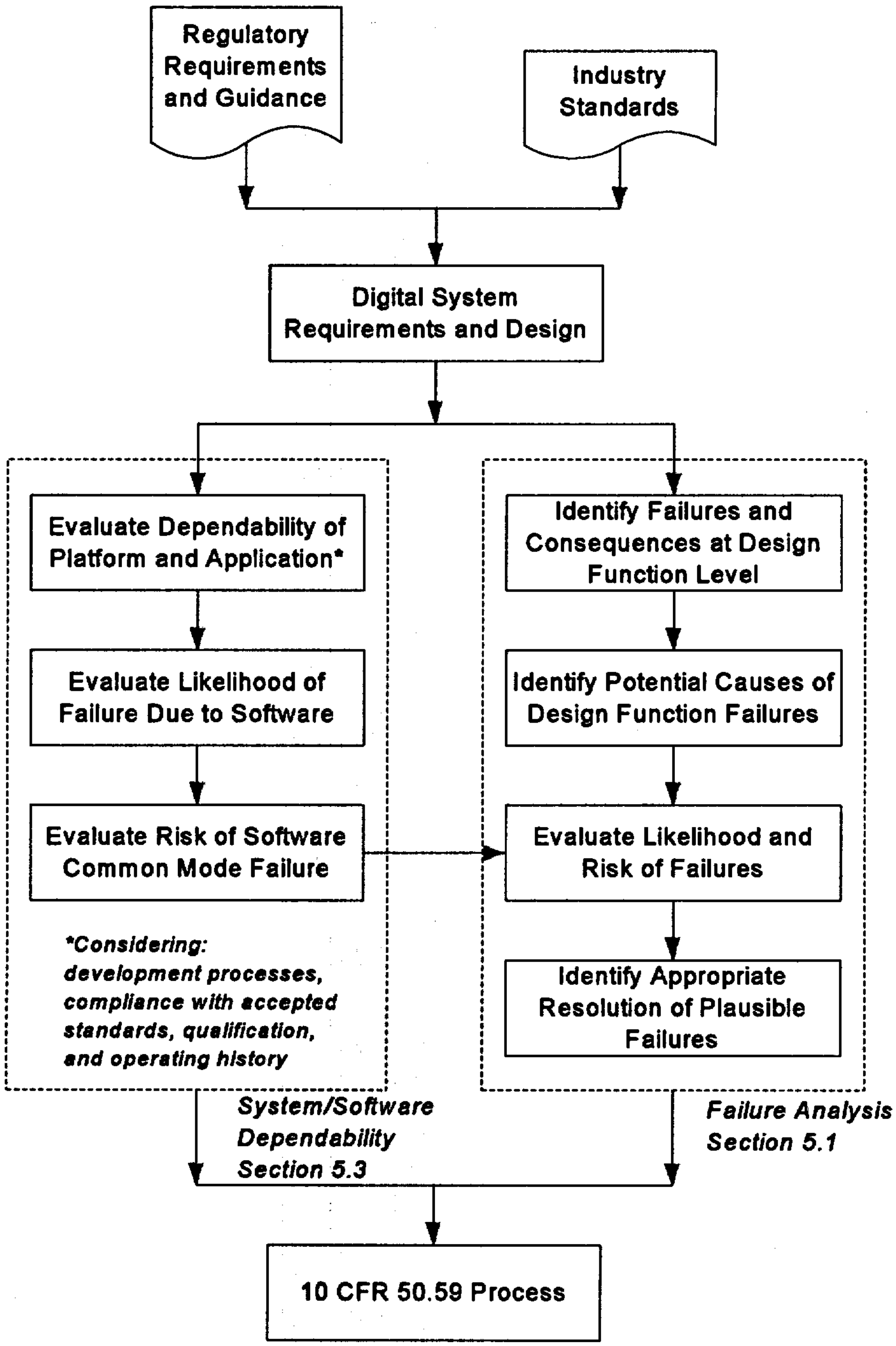



**Figure 4-2**
**Engineering Evaluations in the 10 CFR 50.59 Process**

### 4.1.2 Dependability and Risk of Failure Due to Software

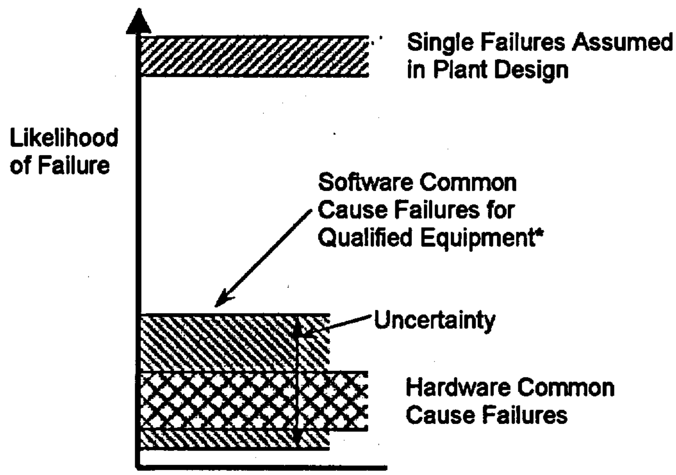
In the Standard Review Plan, Chapter 7, the NRC emphasizes that quality is one of the key defenses against software common cause failure. While the specific probability of failure due to a software design flaw cannot be determined on a quantitative basis, there are established methods for software development and qualification that, when followed, provide reasonable assurance that the likelihood of failure due to software is sufficiently low. To determine whether a digital system poses a significant risk of software failure, the factors that contribute to its dependability (or likelihood of failure) and quality need to be evaluated. The evaluation should consider:

- The development and quality assurance processes applied to both the digital platform itself and the plant-specific application software (see Section 5.3.3). Processes for design, V&V, and configuration control of software should be documented.
- Compliance with industry standards and regulatory requirements and guidelines for design, development and verification of the digital system and its software (see Section 5.3 and Table 5-1).
- Quality assurance per 10 CFR 50, Appendix B applied in the design of the plant-specific system and software application.
- For commercial grade equipment, factors that compensate for lack of documented processes compliant with nuclear industry standards, following the approach in EPRI TR-106439 (see Section 5.3.3.6).
- Existing qualification certifications, including NRC Safety Evaluation Reports documenting review of generic qualification tests and evaluations. While the effort required on the part of the licensee to evaluate the platform is reduced by virtue of the prior NRC review, the licensee will still need to evaluate the plant-specific application and implement plant-specific action items identified by the NRC as a result of their review.

This list is not all-inclusive and is only intended to serve as a guide in the evaluation of the quality of the digital device. Section 5 provides detailed guidance on addressing digital upgrade issues that relate to the quality of the upgrade and thus the likelihood of failure due to software. Additional factors that can contribute to the determination that the likelihood of software common cause failure is acceptably low include:

- The maturity of the product and substantial, relevant history of satisfactory operation in similar applications (including operating experience at other plants and in other industries). Additional confidence is gained if the same equipment and application program have been used successfully in other nuclear plants or other similar applications.
- Simple software architecture, few inputs/outputs, well-defined failure states, built-in fault tolerance (see Section 5.3.2). Systems that are sufficiently simple can have well defined failure modes and tend to allow for more thorough testing of all input and output combinations than complex systems. The simplicity of the digital equipment itself and of the application should be considered.

In considering digital upgrades in the context of 50.59, there should be reasonable assurance that failures due to software, particularly common cause failures in redundant channels, are sufficiently unlikely. However, it is typically difficult to obtain further assurance that the likelihood of common mode failure due to software is as low as that for hardware, even when the software is designed in accordance with a 10 CFR 50, Appendix B process. As a result, there may be a larger uncertainty associated with determining the likelihood of failure due to software relative to other types of failures, as depicted below.




* Note: For digital equipment shown to be of high quality, the likelihood of software common cause failure is expected to be much less than the likelihood of single failures assumed in plant design.

**Figure 4-3**
**Likelihood of Common Cause Failures due to Hardware and Software**

## 4.2 Applicability of 10 CFR 50.59

Section 4.1 of NEI 96-07, Revision 1, provides guidance on the applicability of 10 CFR 50.59. In some cases, a change may be controlled by more specific regulations. Also, for digital-to-digital changes that appear to be like-for-like replacements, an equivalency evaluation should be performed to determine if the replacement is a plant design change (subject to 10 CFR 50.59) versus a maintenance activity. Digital-to-digital changes may not necessarily be like-for-like because the system behaviors, response time, failure modes, etc. for the new system may be different from the old system. If the vendor, hardware, firmware, application software, and configuration data are identical, then the upgrade may be a like-for-like maintenance activity where 10 CFR 50.59 would not apply.

### *4.2.1 Review for Potential Tech Spec Changes*

If the planned upgrade involves a change to the Technical Specifications, then the licensee submits a request for amendment to the facility license in accordance with the provisions of 10 CFR 50.90. The NRC reviews and needs to approve the Technical Specification change prior to implementation of the plant modification. The submittal should concentrate on those aspects of the modification that result in the Technical Specification change.

Reviews to determine whether digital upgrades involve Technical Specification changes should cover the items listed below:

- Safety limits, limiting safety system settings, and limiting control settings. These are limits on important process variables that are necessary to reasonably protect the integrity of the physical barriers that guard against the uncontrolled release of radioactivity.
- Limiting conditions for operation. These are the functional capabilities or performance levels of equipment required for safe operation of the facility.
- Surveillance requirements. These are requirements relating to test, calibration, or inspection to assure that the necessary quality of systems and components is maintained, that facility operation will be within the safety limits, and that the limiting conditions of operation will be met.
- Design features. Design features are those features of the facility such as channel accuracy and time response which, if altered or modified, could have a significant effect on safety.
- Administrative controls. These provisions relate to organization and management, procedures, record keeping, review and audit, and reporting necessary to assure operation of the facility in a safe manner.

The review should consider the bases for the Technical Specifications and applicable plant Safety Evaluation Reports (SERs) to determine if any changes to the Technical Specifications are needed or if a new Technical Specification is needed per 10 CFR 50.36. It should consider in particular any parameters, assumptions or testing requirements that may have been unique to the system or equipment being replaced and no longer apply with the digital upgrade. Also, it should include consideration of parameters, assumptions, or testing requirements unique to the digital system or equipment that were not required for the earlier system and need to be added. Additional guidance is provided in EPRI 1001045.

Note that NEI 96-07, Revision 1, states in Section 4.1.1 that it is acceptable to implement setpoint changes affecting Technical Specifications in a license amendment pursuant to 10 CFR 50.90 while the remainder of the associated modification is implemented under the 10 CFR 50.59 process.

## 4.3 50.59 Screening

In accordance with 10 CFR 50.59, plant changes are reviewed by the licensee to determine whether the change can be made without obtaining a license amendment (i.e., without prior NRC review and approval of the change). The 10 CFR 50.59 process of determining when prior NRC review is required includes two parts: screening and evaluation. The screening process involves determining whether a change has an adverse effect on a design function described in the UFSAR; the evaluation process involves determining whether the change has more than a minimal effect on the likelihood of failure or on the consequences associated with the proposed activity.

The mere fact that a change converts analog equipment or signals to digital does not cause the change to screen in. There are other specific aspects of the change that must be considered in screening which are discussed in this section.

### 4.3.1 Screening Process Overview

Figure 4-4 provides an overview of the thought process involved in 10 CFR 50.59 screening. The first step in screening is to determine whether the change affects a *design function* as described in the UFSAR. If it does not, then the change screens out, and can be implemented without further evaluation under the 10 CFR 50.59 process. If the change does affect a UFSAR-described design function, then it should be evaluated to determine if it has an *adverse effect*. Changes with adverse effects are those that have the potential to increase the likelihood of malfunctions, increase consequences, create new accidents, or otherwise meet the 10 CFR 50.59 evaluation criteria. Additional guidance on the definition of *adverse* is provided in the bulleted examples in Section 4.2.1 of NEI 96-07, Revision 1. These include:

- Decreasing the reliability of a design function,
- Adding or deleting an automatic or manual design function,
- Converting a feature that was automatic to manual or vice versa,
- Reducing redundancy, diversity, or defense-in-depth, or
- Adversely affecting the response time required to perform required actions.

If a change is adverse, then a 10 CFR 50.59 evaluation is performed to determine whether the specific criteria provided in 10 CFR 50.59(c)(2) are satisfied.

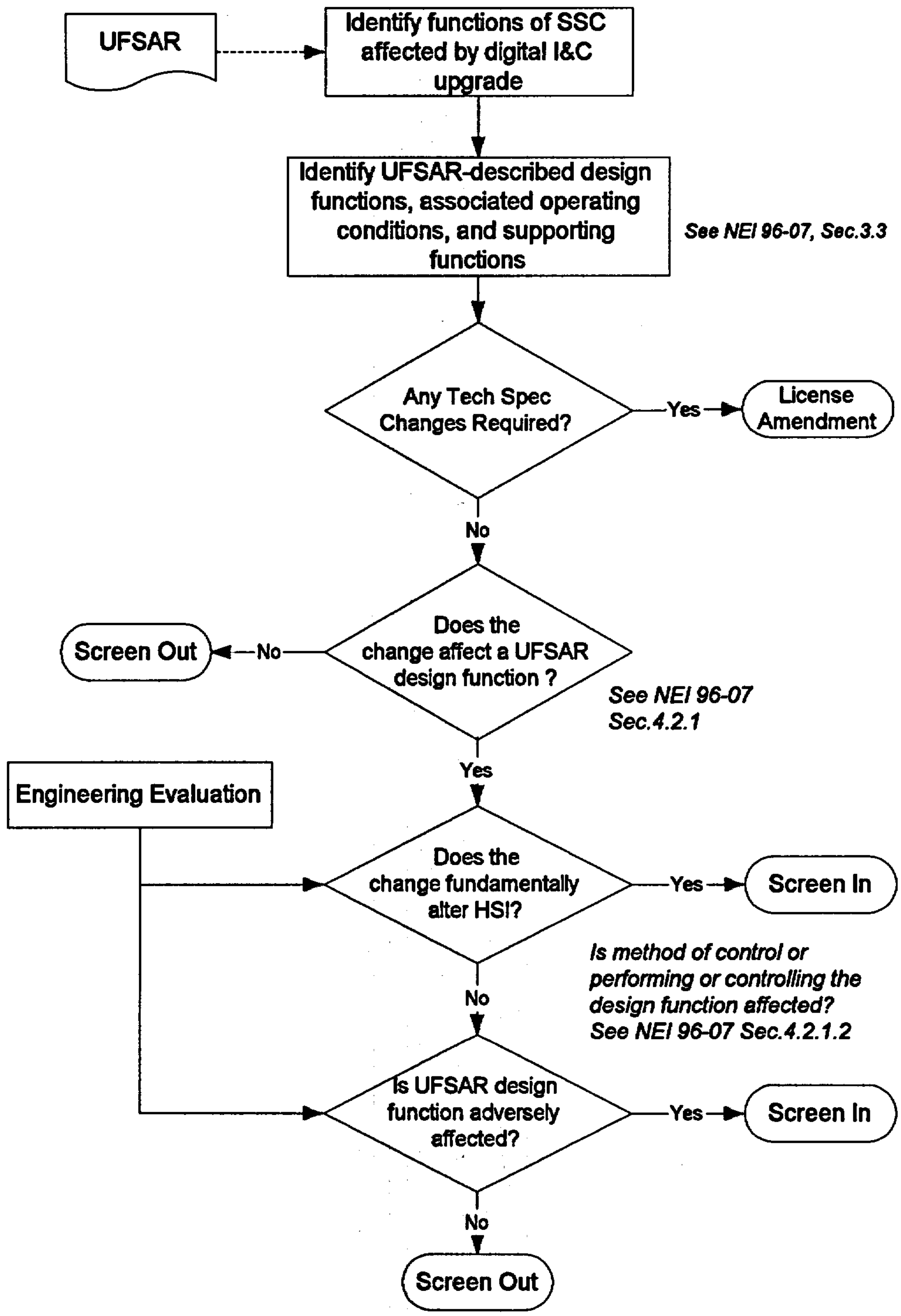



**Figure 4-4**
**10 CFR 50.59 Screening**

### 4.3.2 Software Considerations

With respect to screening digital upgrades, one important question is whether adverse effects are created by software. An adverse effect may be the potential marginal increase in likelihood of failure due to the introduction of software. For redundant safety systems, this marginal increase in likelihood creates a similar marginal increase in the likelihood of a common failure in redundant channels. On this basis, most digital upgrades to redundant safety systems should be conservatively treated as "adverse" and screened in for further evaluation under the 10 CFR 50.59 process.

However, for some relatively simple digital equipment, engineering evaluations may show that the risk of failure due to software is not significant and need not be evaluated further, even in applications of high safety significance. As described in Section 5, consensus methods have been developed for evaluating dependability of digital equipment including assessment of the potential for common cause failure due to software. Overall, the ability to evaluate the dependability of digital equipment has improved over the years, as some vendors are using updated and improved processes for software and digital system development, V&V and configuration management. Also, some digital equipment has gained extensive operating history, both inside and outside the nuclear industry.

Thus, for some upgrades the likelihood of failure due to software may be judged to be no greater than failure due to other causes, i.e., comparable to hardware common cause failure. In such a case, even when it affects redundant systems, the digital upgrade would screen out. Example 4-1 describes the case of a digital "smart" transmitter that uses a relatively simple digital architecture internally, drives the existing 4-20 mA instrument loop, has limited functionality that can be comprehensively tested, and has extensive operating history.

*Example 4-1. Screening for a Smart Transmitter (Screens Out)*

Transmitters are used to drive signals for parameters monitored by redundant ESFAS channels. The original analog transmitters are to be replaced with microprocessor-based transmitters. The firmware in the new transmitters implements a simple process of acquiring one input signal, setting one output, and performing some simple diagnostic checks. This process runs in a continuous sequence with no branching or interrupts. An alarm relay is available to annunciate detected failures. For each channel, the existing 4-20 mA instrument loop is maintained without any changes other than replacing the transmitter itself.

An engineering evaluation of the new device concludes that it has been developed in accordance with a well-defined life cycle process that complies with industry standards and regulatory guidance. In addition, based on the simplicity of the device (one input and two outputs), it was easily tested. Further, substantial operating history has demonstrated high reliability in applications similar to the ESFAS application. Failures are bounded by existing failures of the analog device (see Section 5.1 for further discussion of failures), and the likelihood of concurrent failures in multiple channels is considered to be very low (e.g., less than the likelihood of common mode failures due to maintenance or calibration errors), and falls within the "negligible risk" region of Figure 3-2. Consequently, it is concluded that no adverse effects are created, and the change screens out.

Note that an upgrade that is similar to Example 4-1, but that uses digital communications from the smart transmitter to other components in the instrument loop might screen in because new interactions and potentially new failure behaviors are introduced that could have adverse effects and should be analyzed in a 10 CFR 50.59 evaluation (see Example 4-2).

*Example 4-2. Screening for a Smart Transmitter (Screens In)*

Smart transmitters similar to those described in Example 4-1 are to be installed as part of an upgrade to the reactor protection system. The new smart transmitters have the capability to transmit their output signal using a digital communication protocol. Other instruments in the loop are to be replaced with units that can communicate with the transmitter using the same protocol. Because this change not only upgrades to a digital transmitter, but also converts the instrument loop to digital communications among devices, there would be the potential for adverse effects owing to the digital communication and possible new failure modes involving multiple devices. As a result, this change screens in.

### *4.3.3 Other Digital Issues in the Screening Process*

In addition to the software question, other characteristics of a digital upgrade could cause the change to screen in to a 10 CFR 50.59 evaluation. Some potentially adverse effects that should be evaluated when screening digital upgrades include:

- Combining previously separate functions into one digital device such that failures create new malfunctions (i.e., multiple functions are disabled if the digital device fails).
- Changing performance from UFSAR-described requirements (e.g., for response time, accuracy, etc.).
- Changing functionality in a way that increases complexity, potentially creating new malfunctions.
- Introducing different behavior or potential failure modes (for which the risk is not negligible) that could affect the design function.

Examples 4-3 and 4-4 illustrate typical screening considerations for a small digital upgrade.

*Example 4-3. Screening for a Recorder Upgrade (Screens Out)*

An analog recorder is to be replaced with a new microprocessor based recorder. The recorder is used for various purposes including Post Accident Monitoring, which is an UFSAR-described design function. An engineering/technical evaluation performed on the change determined that the new recorder will be highly dependable (based on a quality development process, testability, and successful operating history) and therefore, the risk of failure of the recorder due to software is considered very low. The new recorder also meets all current required performance, HSI, and qualification requirements, and would have no new failure modes or effects at the level of the design function. The operator will use the new recorder in the same way the old one was used, and the same information is provided to support the Post Accident Monitoring function, so the method of controlling or performing the design function is unaltered. The licensee concludes that the change will not adversely affect any design function and screens out the change.

***Example 4-4. Screening for a Recorder Upgrade (Screens In)***

Similar to Example 4-3, a licensee is planning to replace an analog recorder with a new microprocessor based recorder. However, in this instance, the engineering/technical evaluation determined that the new recorder does not truly record continuously. Instead it samples at a rate of 10 hertz, then averages the 10 samples and records the average every one second. This frequency response is lower compared to the original equipment and may result in not capturing all process variable spikes or short-lived transients. In this case, the licensee concludes that there could be an adverse effect on an UFSAR-described design function and screens in the change. In the 10 CFR 50.59 evaluation, the licensee will evaluate the magnitude of this adverse effect.

### 4.3.4 Screening Human-System Interface Changes

In the discussion of the screening process regarding performing or controlling design functions, NEI 96-07, Revision 1, Section 4.2.1.2, states that:

> For purposes of 10 CFR 50.59 screening, changes that fundamentally alter (replace) the existing means of performing or controlling design functions should be conservatively treated as adverse and screened in. Such changes include replacement of automatic action by manual action (or vice versa), changes to the man-machine interface, changing a valve from "locked closed" to "administratively closed" and similar changes.

It is important to note that not all changes to the human-system interface fundamentally alter the means of performing or controlling design functions. Some HSI changes that accompany digital upgrades leave the method of performing functions essentially unchanged. Technical evaluations should determine whether changes to the HSI create adverse effects on design functions (including adverse effects on the licensing basis and safety analyses). Characteristics of HSI changes that could lead to potential adverse effects may include, but are not limited to:

- Changes to parameters monitored, decisions made, and actions taken in the control of plant equipment and systems during transients,
- Changes that could affect the overall response time of the human/machine system (e.g., changes that increase operator burden),
- Changes from manual to automatic initiation (or vice versa) of functions,
- Fundamental changes in data presentation (such as replacing an edgewise analog meter with a numeric display or a multipurpose CRT where access to the data requires operator interactions to display), or
- Changes that create new potential failure modes in the interaction of operators with the system (e.g., new interrelationships or interdependencies of operator actions and plant response or new ways the operator assimilates plant status information).

If the HSI changes do not exhibit these characteristics, then it may be reasonable to conclude that the "method of performing or controlling" the design function is not adversely affected. Note, however, that these characteristics focus on potential adverse effects due to changes in the physical operator interface, not procedure changes. Changes in procedures that may be required in order to implement HSI changes also need to be screened.

With respect to creation of new potential failure modes, changes to the HSI should be treated in a manner similar to software and digital equipment. Specifically, a disciplined development process in which human factors issues are considered by qualified personnel and evaluated using human factors verification and validation techniques should be credited for minimizing the likelihood of human errors and inadvertently introducing a new behavior or problem that did not previously exist for the old device. Section 5.3.4.2 provides guidance on human factors considerations for design and failure analysis.

As an example, if replacement of an analog control system with a digital control system introduces additional automation that alters the required operator response to a transient (for example, a valve automatically shuts as opposed to being shut by operator action), then the "method of performing or controlling" the safety function is changed and a 10 CFR 50.59 evaluation is required. Example 4-5 illustrates another type of fundamental change that screens in.

On the other hand, replacement of a strip chart recorder with a digital, paperless recorder might screen out so long as the data presentation is similar, the recorder location is unchanged, the data displayed is at least as legible as the strip chart recorder was, and the operator uses the recorder in the same way to perform the design function. Therefore, there is no fundamental change in the method of performing or controlling the design function. (This was the conclusion reached earlier in Example 4-3.)

*Example 4-5. Human-System Interface Change (Screens In)*

Component controls for a redundant safety-related system are to be replaced with PLCs. The existing HSI for these components is made up of redundant hard-wired switches, indicator lights, and analog meters. The new system consolidates the information and controls on two flat panel displays (one per redundant train), each with a touch screen providing "soft" control capability.

The flat panel can present any of several selectable display pages, depending on what the operator is doing (e.g., starting/initiating the system, monitoring the system during operation, or changing the system line-up). To operate a control, the operator must (via the touch screen) select the appropriate display page, select the component to be controlled, select the control action (e.g., start or stop), and execute it.

The new HSI will provide better support of operator tasks and reduced risk of errors due to:

- Consolidation of needed information onto a single display that provides a much more effective view of system operation when it is called into action.
- Elimination of the need for the operator to seek out meter readings or indications, saving time and helping to prevent errors.
- Integration of cautions and warnings with the display to help detect and prevent potential errors in operation (e.g., warnings about incorrect system lineup during a test).

However, potential adverse effects include:

- Increased time required to perform some control actions, due to the need to call up the appropriate display and operate the "soft" control.
- Fundamental change in the way information is presented to the operator, and different means of interacting with the controls and indications.

The design was developed using a human factors engineering design, with a verification and validation process consistent with current industry and regulatory standards and guidelines. The goal of the design is to provide a more effective HSI that is less prone to human error than the existing design. However, because of the possible adverse effects noted above, the change is conservatively screened in and will undergo a 10 CFR 50.59 evaluation.

## 4.4 10 CFR 50.59 Evaluation

Section 4.3 of NEI 96-07, Revision 1, presents the eight 10 CFR 50.59 evaluation criteria in the form of questions and provides general guidance on addressing each question. Supplemental guidance specific to digital upgrades is discussed below.

If the evaluation shows that any of the 10 CFR 50.59 criteria are not met, the licensee submits a license amendment request to the NRC and needs to receive approval prior to implementation. If the modification uses a design that was approved previously by the NRC or references a design previously approved by a topical report evaluation, the submittal should focus on application-specific features (i.e., conditions of approval identified in the NRC Safety Evaluation Report) or differences from the previously approved implementation.

### 4.4.1 Does the activity result in more than a minimal increase in the frequency of occurrence of an accident?

The first step in addressing this criterion is to identify the accidents that have been evaluated in the UFSAR and that may be affected by the proposed activity. Then the change is evaluated to determine whether the frequency of these accidents could increase as a result of the change. In answering this question for digital upgrades, the key issue is whether the digital equipment can increase the frequency of initiating events that lead to accidents, considering the following:

- Does the system automate some aspect of plant operation that could relate to accident initiators?
- Does the system exhibit performance or dependability characteristics that increase the need for operator intervention or increase operator burden to support operation of the system in normal or off-normal conditions?
- Could this increase the probability of an accident previously evaluated?

Per Section 4.3.1 of NEI 96-07, the licensee may use PRA calculations to assess the change in probable frequency of events (see Example 5-3). Note that "more than a minimal increase" means greater than 10 percent. The qualitative nature of assessing the likelihood of software failures could be augmented by risk insights gleaned from PRA analyses.

Also, NEI 96-07 states that a change is considered to have a negligible effect on the frequency of occurrence of accidents when the change is so small or the uncertainties in determining whether a change has occurred are such that it cannot be reasonably concluded that the frequency has actually changed. As newer equipment is expected to be more reliable than the equipment it is replacing, a digital upgrade would not be expected to result in more than a minimal increase in the frequency of occurrence of an accident. Results of engineering evaluations regarding the quality, dependability, and qualification of the system (e.g., as discussed in Section 4.4.2, below) should be used in this evaluation.

### 4.4.2 Does the activity result in more than a minimal increase in the likelihood of occurrence of a malfunction of an SSC important to safety?

The issue here is to determine whether the proposed change can cause potential failures of structures, systems, and components (SSCs) to perform their design function as described in the UFSAR.

<u>Level of Detail.</u> In the context of this question, the SSC under consideration depends on the level of detail described in the UFSAR. If the relevant design functions are described in terms of the system in which the digital device is installed, then the system is the SSC. If the UFSAR describes the design functions in terms of the component that the digital device is replacing, then the new digital device is the SSC under consideration in this question.

When evaluating the effect of the proposed change on potential failures, NEI 96-07, Revision 1, states that the level of detail in the evaluation should be consistent with the level of detail of failures or failure modes and effects analysis (FMEA) described in the UFSAR. Thus, if the UFSAR describes potential failures at the plant system level, at the channel or train level, or at the subsystem level, then that is the appropriate level of detail for evaluating the answer to this question.

<u>Likelihood of Malfunctions.</u> It is important to note that although failure of digital equipment is plausible, the likelihood of such failures causing malfunctions of the system in which the equipment is installed may be minimal and might not affect the licensing basis of the plant. In determining likelihood, NEI 96-07, Revision 1, states in Section 4.3.2 that:

> Qualitative engineering judgment and/or an industry precedent is typically used to determine if there is more than a minimal increase in the likelihood of occurrence of a malfunction.

And:

> A proposed activity is considered to have a negligible effect on the likelihood of a malfunction when a change in likelihood is so small or the uncertainties in determining whether a change in likelihood has occurred are such that it cannot be reasonably concluded that the likelihood has actually changed (i.e., there is no clear trend toward increasing the likelihood).

The failure analysis (Section 5.1) is needed to understand how potential failures of the digital upgrade affect the system in which it is installed, and whether digital device failures can cause the system to fail to perform its design function. The failure analysis should also provide the insights needed to determine if the change reduces redundancy, diversity, separation, or independence, which are considered to result in more than a minimal increase in the likelihood of occurrence of malfunctions.

Evaluations of the dependability of the system (Section 5.3) are needed to assess whether the likelihood of malfunctions has increased. In many cases, digital upgrades are installed to replace obsolete and/or unreliable equipment that has become costly to maintain. If actual failure rate data are available for the old equipment and the replacement equipment, it may be used to evaluate the change in hardware reliability. Typically, digital hardware is more reliable than the equipment it replaces. Also, modern digital equipment designed for safety significant applications often incorporates important design features that contribute to a lower likelihood of malfunction. Such features can improve the dependability of a train of a system; thus preserving the system-level design function. These features should be credited in the 10 CFR 50.59 evaluation, and may include:

- Internal redundancy and fault tolerance to preclude single faults from causing the device to malfunction.
- Self-diagnostics to detect and alarm faults, or abnormal or unanticipated conditions so that operators can take timely corrective action before the system is called upon to perform its design function. Of course, good self-diagnostics should be coupled with an effective corrective action program at the plant.

- Self-test routines that perform surveillance testing functions on a more frequent basis than the original, manually executed surveillance tests.

**Design, Qualification and Compliance with Standards.** While it is expected that newer equipment will be more reliable than the equipment it is replacing, other issues that should be addressed are compliance with applicable regulations and industry standards; qualification for environmental conditions (seismic, temperature, humidity, radiation, pressure, and EMC); performance requirements for the plant-specific application; proper design of electrical power supplies; cooling or ventilation for thermal loads; and separation, independence and grounding.

**Malfunctions due to Software.** As discussed above in Section 4.1, the question of whether software increases the likelihood of malfunctions is addressed in the design process by evaluating various characteristics of software that relate to the quality of the system. A digital device developed in accordance with a defined life cycle process, complying with the applicable industry standards and regulatory guidance discussed in Section 5 should not result in more than a minimal increase in the likelihood of malfunctions. This is illustrated in Example 4-6.

On the other hand, other aspects of the upgrade could cause a licensee to conclude that there is more than a minimal increase in the likelihood of malfunction. For example, a license amendment request could be required as a result of a reduction in system performance (e.g. response time, accuracy) or degrading the environment (e.g. EMI, temperature, humidity, seismic, airborne particulates) such that there is more than a minimal increase in the likelihood of malfunction of an SSC important to safety.

***Example 4-6. Likelihood of Malfunctions for a PLC Upgrade***

The existing, obsolete load sequencer in each of two redundant ESFAS trains will be replaced using PLCs that have been "pre-qualified" for use in safety-related applications. Based on their evaluation of the PLC platform, including hardware design and qualification and software development, V&V, and configuration control, the NRC concluded in a Safety Evaluation Report (SER) that the PLC is acceptable as a platform for safety-related applications. Additional plant-specific action items identified in the SER have been addressed by the licensee in the sequencer design as appropriate.

The plant-specific application software is straightforward (essentially limited to replication of several time delay functions and simple logic), and replicates the functionality of the existing system. The application software was developed under a 10 CFR 50, Appendix B, QA program using software life cycle, V&V, and configuration control processes that comply with accepted industry standards and regulatory guidance.

The design of the system hardware and software includes redundant components for fault tolerance and self-diagnostic features that identify and alarm hardware faults and interruptions in the normal processing routines. The integrated load sequencer system was tested to validate all system requirements and to confirm appropriate system behavior in the presence of plausible abnormal conditions and events. No unexpected behavior was observed during testing.

The 10 CFR 50.59 evaluation concludes that the dependability of the system (based on pre-qualification of the platform and use of accepted methods for developing and validating the application) provides reasonable assurance that malfunctions, including common cause failure due to software, will be highly unlikely, and much less likely than other malfunctions presently considered in the UFSAR. Therefore, the change would not cause more than a minimal increase in likelihood of malfunctions.

***Example 4-7. Likelihood of Malfunctions due to Reduction In Performance***

The reactor protection system in a Boiling Water Reactor (BWR) plant is to be replaced with a digital system. The new digital system is expected to provide increased reliability through more reliable digital hardware and fault tolerance, plus built-in self-diagnostics that will ease compliance with maintenance and surveillance requirements. However, evaluation of system performance shows that, although it is acceptable, the response time is slower than that of the existing system. The reactor pressure trip function has a requirement to respond very quickly to increases in reactor vessel pressure because in a BWR, there is a strong relationship between pressure and void fraction, and therefore reactivity. Because the response time of the digital system would be slower than that of the original analog system, and exceeds the licensing basis requirements in the UFSAR, a License Amendment is required to implement this change. The LAR would describe results of revised safety analyses in which the reactor pressure trip function is shown to adequately protect the plant even with the increased response time of the new equipment.

### 4.4.3 Does the activity result in more than a minimal increase in the consequences of an accident?

Per NEI 96-07, Revision 1, "increases in consequences" refers to an increase in potential radiological dose from an accident. In evaluating this criterion, the first step is to determine which accidents evaluated in the UFSAR may have their radiological consequences affected as a direct result of the proposed activity.

If the system does not directly contribute to accident prevention or mitigation, then a digital upgrade to the system will not likely increase the consequences of an accident.

### 4.4.4 Does the activity result in more than a minimal increase in the consequences of a malfunction?

Again, the system's safety significance and the PRA should indicate whether it is important for preventing or mitigating radiological consequences.

If the system does play a role in mitigating the radiological consequences of accidents, then it is important to determine whether the change can cause malfunctions that affect the mitigation function such that consequences are increased. The results of the evaluation of Criterion 6 will help by showing if the change introduces any malfunctions with results different from those previously analyzed in the UFSAR. If the results of malfunctions are no different, then there is not likely to be any increase in consequences of accidents.

### 4.4.5 Does the activity create a possibility for an accident of a different type?

When addressing this question, the types of accidents that have been evaluated in the UFSAR need to be identified and a determination made as to whether the proposed activity could create accidents that are not bounded by UFSAR-evaluated accidents. The evaluation should consider whether the change creates new events that can initiate accidents that are of a different type than those evaluated in the UFSAR. The answers to the following questions should assist in identifying accidents of a different type:

- Have the assessments of system-level potential failure modes and effects for the new system or equipment identified any new types of system-level failure modes that could cause a different type of accident than presented in the UFSAR?
- Plant UFSAR analyses were based on credible failure modes of the existing equipment. Does the replacement system change the basis for the most limiting scenario?

### *4.4.6 Does the activity create a possibility for a malfunction of an SSC important to safety with a different result?*

This question addresses results or effects of potential system failures, and whether the effects are bounded by failures explicitly described in the UFSAR. The evaluation needs to compare results of malfunctions evaluated in the UFSAR with the results of failures that the proposed activity could create. The key issue is the effect of failures of the digital device on the system in which it is installed. The failure analysis (Section 5.1) will provide insights to system failures and their effects on SSCs. If failures of the digital device cause the system to malfunction (i.e., not perform its design function), then the evaluation needs to determine if the result of the system malfunction is bounded by or different than those previously evaluated.

Note that new types of malfunctions are not the issue. NEI 96-07, Revision 1, states that "a new failure mechanism is not a malfunction with a different result if the result or effect is the same as, or is bounded by, that previously evaluated in the UFSAR."

As an example, NEI 96-07, Revision 1, notes that a digital feedwater control system upgrade may add new components that can have failure modes different than the original components. Provided the end result of the control system failure is bounded by the results of malfunctions already evaluated in the UFSAR (e.g., loss of feedwater), this upgrade would not create malfunctions with a different result.

**Level of Detail**. As discussed above for 10 CFR 50.59 Criterion 2 (Section 4.4.2), the evaluation needs to consider the level of detail that was previously evaluated in the UFSAR (i.e., component versus division/train versus system level failures). Another way to determine the appropriate level of detail is to consider the level at which design functions are described in the UFSAR. If the relevant design functions are assigned at the system level, then it is appropriate to evaluate the effects of malfunctions at this level.

**Types of Malfunctions.** The key in evaluating the change is to determine the set of failures that are plausible at the appropriate level of detail, and whether they could disable the design function. In Section 4.3.6, NEI 96-07, Revision 1, states:

> a proposed activity that introduces a cross-tie or credible common mode failure (e.g., as a result of an analog to digital upgrade) should be evaluated further to see whether new outcomes have been introduced.

And:

> The possible malfunctions with a different result are limited to those that are as likely to happen as those described in the UFSAR. For example, a seismic induced failure of a component that has been designed to the appropriate seismic criteria will not cause a malfunction with a different result. However, a proposed change or activity that increases the likelihood of a malfunction previously thought to be incredible to the point where it becomes as likely as the malfunctions assumed in the UFSAR could create a possible malfunction with a different result.

Hence, for the purpose of the 10 CFR 50.59 evaluation, "credible" malfunctions are defined as those as likely as the malfunctions already assumed in the UFSAR. As discussed in Section 3.2.2, failures due to design errors are not evaluated in the UFSAR and need not be considered as potential malfunctions since they are minimized through control of the design process.

Results of the failure analysis should be used to identify the effects on the design function of failures that are as likely as those in the UFSAR. The effects of these failures should be compared to the failures addressed or assumed as part of the safety analyses in the UFSAR. If there is reasonable assurance that potential failures are not as likely as those described in the UFSAR, then such failures do not merit further consideration in the 10 CFR 50.59 evaluation.

For failures that are deemed as likely as the malfunctions in the UFSAR, the failure analysis performed during the design effort is used to "see whether new outcomes have been introduced." If the failure analysis shows that using only existing equipment and procedures, and with only minor procedural changes, there would be adequate backups to mitigate potential adverse impacts on design functions, then for the purposes of the 10 CFR 50.59 evaluation, there would be no new outcome, and the change would be implemented under 10 CFR 50.59. The 10 CFR 50.59 evaluation would document the basis of this conclusion, along with any licensing commitments needed to ensure the future functionality of the back up.

<u>Software Common Cause Failures</u>. Engineering evaluations of the quality and design processes determine if there is reasonable assurance that the likelihood of failure due to software is sufficiently low. In this evaluation, "sufficiently low" means much lower than the likelihood of failures that are considered in the UFSAR (e.g., single failures) and comparable to other common cause failures that are not considered in the UFSAR (e.g., design flaws, maintenance errors, calibration errors). Results of this evaluation are then used to determine whether failures due to software, including common cause failures, should be considered further in the 10 CFR 50.59 evaluation. If there is reasonable assurance that the likelihood of failure due to software is sufficiently low, then the upgrade would not require prior NRC review on the basis of software common cause failures (see Example 4-8).

*Example 4-8. Results of Malfunctions for a PLC Upgrade*

The load sequencer in Example 4-6 monitors the 1E electrical distribution system voltage and sheds loads in response to an undervoltage condition, allowing the EDGs to come to rated speed and voltage. Loads are then sequenced back on line based on the ESF actuation signals provided to the sequencer from the ESFAS logic system. All ESF actuation signals are processed by the load sequencer so that if the sequencer fails, no ESF equipment will start.

A FMEA of the PLC system identified a limited number of possible single failures that are not detected by the system, but that can be detected by application-specific design features. In the design of the sequencer application, additional failure analysis was performed and results were used in the design to reduce the consequences of certain postulated failures.

In addressing Criterion 2, the quality, dependability, and enhanced capabilities of the digital system are evaluated in the context of the evaluation. The upgrade uses a pre-qualified PLC platform that has been shown to be a high quality, highly dependable system, as documented in an SER summarizing the review performed by the NRC. In a comparison to the equipment being replaced, it is shown that many hardware vulnerabilities have been eliminated, and self-test and diagnostic capabilities have been added. The qualitative assessment concludes that the net result is a decrease in the likelihood of failure of the system, so that the "minimal increase" threshold of Criterion 2 has not been challenged.

In addressing Criterion 6 in regard to potential software common cause failures, both the embedded software in the PLC and the application-specific or "configuration" software are considered. Evaluations performed during the pre-qualification efforts established assurance that the quality of the embedded software is such that the likelihood of failure is acceptably low. The application-specific software has been developed and tested under Appendix B QA processes, utilizing configuration tools that are designed specifically to minimize the likelihood of introducing errors. The conclusion of the qualitative assessment is that the likelihood of a software common cause failure is much less than that of other events considered in the UFSAR and therefore software common cause failure is not considered a possible malfunction with a different result (as discussed in NEI 96-07, Revision 1).

**Other Failures.** In addition to failures due to software, it is important to note that there may be other effects of a digital upgrade that could create new results of malfunctions (e.g., combining functions, creating new interactions with other systems, changing response time, etc.) and these other effects should also be addressed. For example, if previously separate functions are combined in a single digital device, then the evaluation needs to consider whether single failures that could previously have disabled only individual functions can now disable multiple functions. NEI 96-07 illustrates this concern when it states:

> An example of a change that would create the possibility for a malfunction with a different result is a substantial modification or upgrade to control station alarms, controls, or displays that are associated with SSCs important to safety that creates a new or common cause failure that is not bounded by previous analyses or evaluations.

Of course, if the failure analysis (or defense-in-depth and diversity analysis) showed that other plant design changes or procedure changes were necessary in order to provide back-ups for potential failures, then these additional changes should be considered in the 10 CFR 50.59 evaluation (e.g., the likelihood and results of malfunctions due to these additional changes should also be addressed). Refer to Section 4.3 NEI 9607, Revision 1, for guidance on when multiple changes should be evaluated together. Care needs to be taken, however, because addition of diverse backups when not required could result in a decrease in reliability and safety due to increased complexity and potential for error associated with maintaining and operating diverse equipment.

*Example 4-9. Malfunctions with Different Results*

The original analog RTS and ESFAS Systems are to be replaced with a new digital system. The original design of the system includes four channels of instrument inputs with signal conditioning and bistable comparators for trips on individual signals. These four channels also feed two independent trip logic channels in which two-out-of-four trip logic is implemented to create two independent reactor trip signals. The ESFAS actuation logic is also implemented in two separate and independent trains.
In the new design, four separate and independent processors (each with associated input, output, and communication modules) are used to acquire the RTS instrumentation signals for each of the two separate reactor trip channels. The four RTS instrumentation processors perform conversion to engineering units and replication of the bistable comparisons. Each then communicates via a digital communication link with two separate and independent processors that perform both the RTS trip logic and the ESFAS logic.

The failure analysis determines that a plausible common failure mode is garbled communication between a trip/actuation processor and all four instrumentation processors, affecting the performance of each of the four instrumentation processors (e.g., slowing input acquisition due to increase in communication load). Such a malfunction could affect the function of the redundant trip/actuation processor by slowing the rate at which the input processors can communicate thereby reducing the overall response of the trip/actuation system. This type of malfunction could affect the RTS and ESFAS functions in a way that has not been analyzed in the UFSAR. Thus, the licensee concludes that this modification requires a LAR and can not be implemented under 10 CFR 50.59.

### 4.4.7 Does the activity result in a design basis limit for a fission product barrier being exceeded or altered?

NEI 96-07, Revision 1, notes that the fission product barriers include the fuel cladding, reactor coolant system boundary, and containment, and the design basis limit pertains to the controlling numerical values in the UFSAR used to <u>directly</u> determine the integrity of such fission product barriers.

The first step in addressing this question is to determine if any of the numerical values used are associated with the change. If the design basis limit for the fission product barrier is controlled by another regulation specific to the parameter, then the effect on that limit is examined under the specific regulation. It would be unlikely that a design basis limit would be exceeded or altered as a result of a digital upgrade. However, the design basis limits could be affected if the timing (response time or processing time) of the digital device is different from that of the older analog system. If the change would result in the design basis limit for the parameter being exceeded, then the change would not be implemented under 10 CFR 50.59 and would require prior approval by the NRC. Similarly, if the change includes alteration of the numerical value of the design basis limit, NRC review would be required.

### 4.4.8 Does the activity result in a departure from a method of evaluation described in the UFSAR used in establishing the design bases or in the safety analyses?

This question applies to those analytical methods that are described in the UFSAR and demonstrate that the design meets the design bases or that the safety analysis is acceptable. NEI 96-07, Revision 1, indicates that a change to any element of the analysis methodology that

produces a result that is not essentially the same as the prior analysis, or use of a method of evaluation not already approved by the NRC, constitutes a departure from a method of evaluation described in the UFSAR. Since licensees usually obtain NRC approval for changes to the analytical methods separately from implementing physical plant changes (either under 10 CFR 50.59 or via LAR), it is unlikely that a digital upgrade would involve a departure from a method of evaluation.

## 4.5 License Amendment Process

NEI's white paper "Standard Format for Operating License Amendment Requests From Commercial Reactor Licensees" provides a framework for the license amendment request (LAR). A license amendment submittal will contain the following, as a minimum:

- A summary of the proposed change and technical justification;
- The proposed revision to the Technical Specifications and Bases, if applicable;
- The proposed revision to the Updated Final Safety Analysis Report (UFSAR), if applicable;
- Documentation of the determination that the amendment contains No Significant Hazards Considerations pursuant to 10 CFR 50.92 (see Section 4.5.1);
- Environmental Considerations, documentation of categorical exclusion pursuant to 10 CFR 51.22 (see Section 4.5.2)

Additional documentation that may be helpful for a digital upgrade LAR, but is not required to be included with the formal submittal, includes:

- Defense-in-depth and diversity analysis;
- Technical Specification revision discussion or Technical Specification compliance assessment (if no revision is needed);
- Description of the hardware, firmware, and software;
- Description of verification and validation activities and configuration management process for the new design;
- System testing summary, including discussion of factory acceptance, integration, installation, surveillance, and time response tests;
- Compliance with hardware qualification requirements;
- Operating and maintenance procedures for the new design;

- Description of design development and operational history of vendor's software components; and
- Description of procedures and methodology used by licensee to ensure that the functional design basis is implemented.

Additional guidance for completing the standard format safety analysis provided in the NEI white paper is included below.

### 4.5.1 No Significant Hazards Consideration

Section 4.0 of the NEI white paper addresses the significant hazards consideration, pursuant to 10 CFR 50.92, "Issuance of Amendment", through three questions corresponding to the three criteria in 10 CFR 50.92:

1. Does the proposed change involve a significant increase in the probability or consequences of an accident previously evaluated?

   The first question addresses the same issues presented in the criteria in 10 CFR 50.59(c)(2)(i) and (iii), corresponding to the questions in Sections 4.4.1 and 4.4.3 regarding the probability or consequences of an accident previously evaluated. When considering the effect of the digital upgrade on the probability of an accident, it is important to note the effect the system has on initiating an accident. If the system involved in the digital upgrade can play a part in initiating an accident, the digital device dependability should be evaluated.

   The consequences of an accident refer to the release of radiation dose to the public. Systems that provide accident mitigation functions could affect the consequences of an accident. Consideration should be given to the upgrade's effect on defense-in-depth and backup systems, and system response times.

2. Does the proposed change create the possibility of a new or different kind of accident from any accident previously evaluated?

   This question addresses the same issues presented in the criteria in 10 CFR 50.59(c)(2)(v), corresponding to the question in Section 4.4.5 regarding a new or different kind of accident. Criterion 5 examines the possibility of creating an accident of a different type as a result of the activity. As discussed above, it is important to distinguish between systems that perform monitoring and detection functions and systems that provide active control of the plant to prevent an accident from occurring (such as feedwater or reactor coolant control systems). If the system affected performs accident mitigation functions, then the upgrade will not result in the possibility of a new or different kind of accident. If the system affected does provide active control of the plant, then the potential failure modes of the system as a result of the upgrade should be evaluated.

3. Does the proposed change involve a significant reduction in a margin of safety?

Consideration should be given to the effects the change may have on plant safety limits, setpoints, response times, or design parameters. The focus should be on any decrease in the margin between a regulated design basis limit and the expected failure point associated with that limit and the significance of that decrease. Also, NRC notes in the Federal Register notice regarding the final 10 CFR 50.59 rule that the change does not result in a significant reduction in margin of safety if a change does not result in:

- A design basis limit for a fission product barrier being exceeded or altered (10 CFR 50.59(c)(2)(vii) criteria, or the question in Section 4.4.7) or
- A departure from a method of evaluation described in the UFSAR used in establishing the design basis or safety analysis (10 CFR 50.59(c)(2)(viii) criteria or the question in Section 4.4.8).

### 4.5.2 Environmental Considerations

10 CFR 51.22, "Criterion for categorical exclusion: identification of licensing and regulatory actions eligible for categorical exclusion or otherwise not requiring environmental review," is addressed in Section 5.0 of the NEI white paper. Digital upgrades may be eligible for categorical exclusion from an Environmental Assessment (EA) or Environmental Impact Statement (EIS) under the criteria provided in 10 CFR 51.22(c)(9). Therefore, the statement suggested by the NEI white paper corresponding to 10 CFR 51.22(c)(9) should be used for digital upgrades. The digital upgrade would be eligible for categorical exclusion under this criterion if it does not involve:

1. A significant hazards consideration, as required by 10 CFR 50.92 (see guidance in Section 4.5.1 for No Significant Hazards Consideration).

2. A significant change in the types or significant increase in the amounts of any effluent that may be released offsite.

   The effect of the upgraded system on the type or amount of effluent should be considered. Changes to parameters such as setpoints, measurement accuracy, and response times, or changes to sampling equipment, could potentially have an effect on effluent.

3. A significant increase in individual or cumulative occupational radiation exposure.

Radiation monitoring, reactivity control, and accident mitigation systems affect individual or cumulative occupational radiation exposure. Changes to these systems should consider the effect on radiation exposure.

However, aspects of the license amendment that relate to areas other than the digital upgrade itself may consider the other criteria of 10 CFR 51.22.

# 5 ADDITIONAL GUIDANCE ON ADDRESSING DIGITAL UPGRADE ISSUES

## 5.1 Failure Analysis In Support of Design and Licensing

As discussed in Section 3 and shown in Figure 3-1, consideration of potential system failures and undesirable behaviors should be an integral part of the process of designing, specifying, and implementing a digital upgrade. Consideration of these undesirable events is referred to collectively as failure analysis. Failure analysis interacts with essentially all the main elements of the design process. It provides information needed to support the licensing evaluations as described in Section 4, and it provides the context in which the digital upgrade issues ultimately can be resolved. Failure analysis examines what you do <u>not</u> want the system or device to do.

Failure analysis should not be a stand-alone activity, and it should not generate unnecessary effort or excessive documentation. It is part of the design process, and it can vary widely in scope depending on the extent and complexity of the upgrade. It should be performed as part of plant design procedures and should be documented as a part of the design process. When performed in accordance with a documented plan, failure analysis is an essential part of the software safety analysis, described in Section 5.3.3.5, as applied to the plant-specific application.

The purpose of the failure analysis is to ensure the system is designed with consideration of potential failures and undesirable behaviors such that the risk posed by these events is acceptable. Failure analysis should include the following elements, which are discussed in the subsequent sections:

- Identification of potential system-level failures and undesirable behavior (which may not be technically "failures") and their consequences. This includes consideration of potential single failures as well as plausible common cause failures.
- Identification of potential vulnerabilities, which could lead to system failures or undesirable conditions.
- Assessment of the significance and risk of identified vulnerabilities.
- Identification of appropriate resolutions for identified vulnerabilities, including provide means for annunciating system failures to the operator.

A variety of methodologies and analysis techniques can be used in these evaluations, and the scope of the evaluations performed and documentation produced depends on the scope and complexity of the upgrade. The analysis maintains a focus at the level of the design functions performed by the system, because it is the effects of the failure on the system and the resulting impact on the plant that are important. Failures that impact plant safety are those that could: prevent performance of a safety function of the system, affect the ability of other systems to perform their safety functions, or lead to plant trips or transients that could challenge safety systems.

### 5.1.1 Identification of Potential System-Level Failures and their Consequences

Ultimately, the digital equipment is installed to support overall system requirements, which in turn are necessary to support the plant system-level requirements. This relationship is illustrated in Figure 5-1. It is generally at the plant system level that major functional requirements exist to support plant safety and availability. Consequently, failure analysis should start by identifying the system or "design function" level functions, and examining how the digital equipment can cause these functions not to be performed. This is the "top-down" approach identified in Figure 5-1.

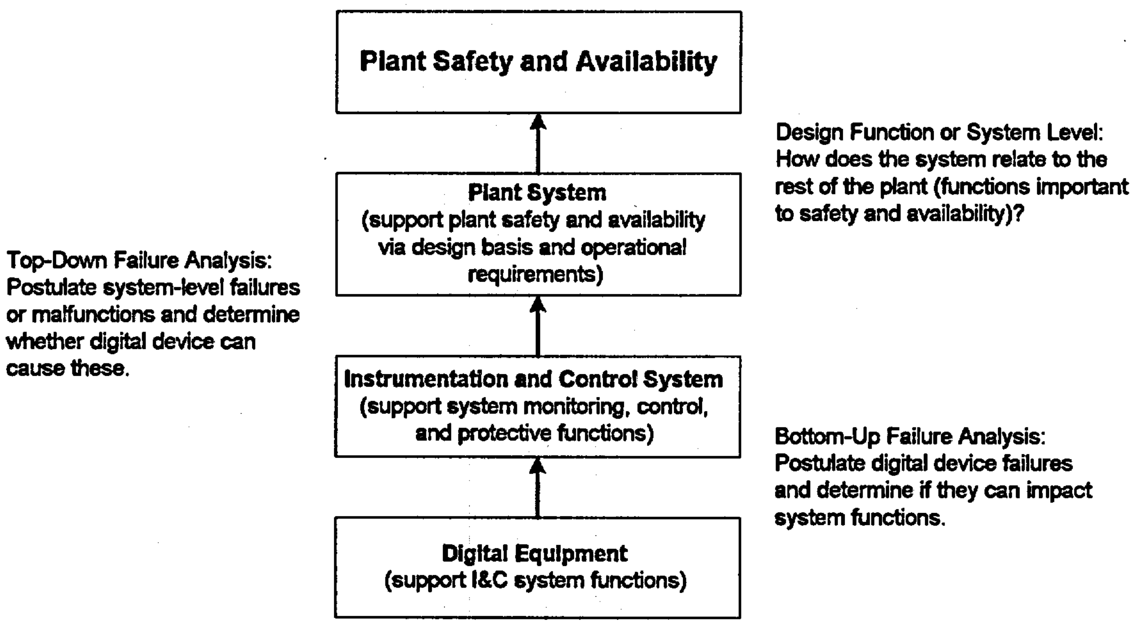



**Figure 5-1**
**Functions and Failures at Different Levels**

In addition to failures of the system to perform its function, other failures such as spurious actions, challenges to safety systems, transient or accident initiators, etc., should be examined. Note that the failures may be not only safety concerns, but also concerns regarding plant availability and investment protection.

It is useful at this stage to review the UFSAR to determine how failures of the affected system are described and analyzed. An understanding of the UFSAR-described failures and their results is needed to support the 10 CFR 50.59 evaluation discussed in Section 4. If the plant design change introduces any failures that cause results different from those analyzed in the UFSAR, then a license amendment may be required.

Example 5-1 illustrates the concept of examining failures at the system level.

***Example 5-1. Examining Failures at the System (Design Function) Level***

Consider an instrument or device that monitors a single input signal and whose only UFSAR-described design function is to drive an output relay that serves as a trip input to a safety system. The safety system latches the trip signal when detected. It also drives a local indicator, but this is not part of a safety function and is not described in the UFSAR. The analog electronic instrument or device is to be replaced with a new, microprocessor-based instrument. It contains firmware which implements the simple trip logic based on the input signal and also provides processing to drive the local indicator. The new device performs exactly the same safety-related trip function as the previous device did, acting through a conventional relay.

Because the device has only a single output that is pertinent to its safety-related function (the relay contact), failures within the device would only affect the safety system through the behavior of the output relay. Therefore, identification of system-level failures is bounded by the failure modes of the output relay. In general, the failure modes of a relay contact output include:

- Fail open (inadvertent opening, failure of the contact in the open position, or failure of the contact to close on demand)
- Fail closed (inadvertent closing, failure of the contact in the closed position, or failure of the contact to open on demand)
- Fail intermittent (contact chatter, cycling, or random state changes).

In this example, assume the relay contact is normally closed and goes to the open position to initiate the trip function. Therefore, it could:

(1) open spuriously, causing an unwanted trip of the system

(2) fail to open when needed (stick in the closed position), preventing a needed trip, or

(3) cycle or chatter, in which case the effect is likely to be a spurious trip (the trip input signal is latched when it is sensed by the system).

These failure modes are bounded by what was considered previously for the analog unit: spurious trip or failure to trip. The licensee determines that although the new device employs a microprocessor and associated software to implement the safety-related function, there are no new failure modes at the system level and therefore no new effects or consequences other than what has been considered previously. This information will be used to support the 10 CFR 50.59 evaluation. (Note that the potential for increasing the likelihood of an already analyzed failure mode also must be considered, and this is discussed in the next example.)

### *5.1.2 Identification of Potential Causes of System Failures*

One purpose of this evaluation of potential causes is to ensure that plausible system-level failure modes have been identified. Looking inside the system for potential failures can help identify system-level effects that may not have been obvious, particularly for a system with multiple inputs and outputs. As such, this step iterates with the first step described in Section 5.1 above.

In order to assess the likelihood of the system-level failures it is necessary to understand the potential causes and their likelihood of occurrence. However, this evaluation should go down only to a level in the design that is necessary to develop confidence that plausible system-level failure modes have been identified and that there is sufficient information to judge the likelihood of the system-level failures. Detailed component-level analyses without a focus on the system level can become overly burdensome, resulting in unnecessary effort and documentation, and can lose sight of the intent of the analysis. Hardware and software analyses may be taken to different levels of detail.

Example 5-2 describes the examination of potential internal failures for a simple digital device and for a more complex computer-based system. It also illustrates how, for a complex system, this examination can identify new results of system-level failures.

Evaluation of the causes of system failures should include consideration of:

- Hardware failures and software errors.
- Failures that may be caused by misoperation of a human-system interface (HSI), either by operators or maintainers.
- Abnormal Conditions and Events (ACEs) as described in Annex F of IEEE 7-4.3.2-1993 and EPRI TR-104595, including EMI-induced failures and other possible external events (e.g., loss of power, loss of environmental control, etc.).
- Failures that may be propagated to other systems through interconnections with external systems (e.g., digital communications).

This evaluation should include consideration of single, multiple, and possible common cause failures (see Sections 3.2.2 and 4.1.2 for guidance on when software should be considered a plausible cause of a common failure). In each case, the failure should be examined further to determine how and when it would be detected.

*Example 5-2. Examination of Internal Failures*

For the microprocessor-based device driving a single output relay described in Example 5-1, the system-level failure modes were bounded by the output relay failure modes, and detailed component-level analyses are not necessary to support failure identification. However, sufficient information should be gathered to assess the likelihood of the identified failure modes. This could be done by examining the internal components or modules and determining likely failure rates based on available failure data for the components (or verifying vendor-supplied data for module failure rates). If the device is a commercial unit with significant operating history, then it may be sufficient to obtain failure rate data for the overall device (e.g., history of failures of the output to operate on demand, history of spurious trip outputs). Operating history may be used to support an argument, but operating history should not be used as the sole method of evaluation. Assessments of the likelihood of failure of the new device compared to the original analog unit are used to support the 10 CFR 50.59 evaluation, specifically the questions related to increased likelihood of malfunctions.

For a more complex system, such as an integrated digital system involving multiple interconnected computers (e.g., distributed, networked computers with a number of inputs, outputs, and interfaces with other systems), identification of plausible failure modes typically will require a more detailed internal examination of the system. The analysis starts at the system level, identifying plausible ways in which the system, its outputs and interfaces could fail and what the consequences are. Then, failures of internal components, modules and communication paths are examined and related to the system outputs to ensure that all potential system-level failures have been identified. For example, examination of faults that could affect a communication path might reveal a combination of system outputs or output failure states that had not been previously identified. Examination of internal failures also supports assessment of the likelihood of the various system-level failure modes. Techniques such as Failure Modes and Effects Analysis (FMEA) and Fault Tree Analysis (FTA) may be used in these evaluations as discussed in IEEE 7-4.3.2-1993 and IEEE 352.

If the more complex system of this example is being used in a large-scale upgrade to a safety system (e.g., reactor protection system or engineered safety features actuation system changeout), and new system-level failure modes are identified that create results different from those previously evaluated in the UFSAR, then a license amendment would be required.

### 5.1.3 Assessment of the Significance and Risk of Identified Failures

The risk posed by a potential failure is determined by its likelihood and the consequences of its effects at the system or plant level. Determining the likelihood of a failure may involve qualitative or quantitative assessments of the probability the failure will occur. In the case of potential hardware failures, methods exist to determine a conservative estimate of reliability and therefore probability of failure.

However, there are no established consensus methods for accurately quantifying reliability of software. Consequently, software failure analysis typically involves making qualitative judgements regarding the dependability of the system (using the considerations discussed in Section 5.3.1) or using conservative bounding levels for failure probability as appropriate. Dependability evaluations are discussed in detail in Section 5.3.

Judgments regarding dependability, likelihood of failures, and significance of identified potential failures should be documented as part of the failure analysis documentation.

Example 5-3 illustrates for a simple device how the likelihood of a software common cause failure can be assessed to determine if this is a significant concern.

***Example 5-3. Assessing the Likelihood of Failures Caused by Software***

Consider a relatively simple device with a single input and single output, such as the one described in Example 5-1, containing a single microprocessor and firmware that implements a simple bistable trip function. Consider the case where two of these will be used in redundant trains to provide the trip function. The device itself is simple, and the software and its structure are examined and determined to be relatively simple and deterministic. The software tools used to build the system are well known and regarded as reliable. The same versions of the software tool have been used for several years to build this application and others. In addition, although complete documentation is not available, the software has been developed and verified and validated using accepted methods. There is extensive operating experience with the software (same version) in applications that also use the device for a bistable function (trip, interlock, or alarm function). There is a mechanism in place for feedback of operating experience and any failures that occur in service, and there have been no failures attributed to software. Based on this information, the likelihood of a software failure is considered extremely small. Given the probabilities of other failures which would lead to the same system-level effects as a software failure (e.g., loss of power or failure of the input signal), failures caused by software errors are judged to be very low likelihood compared to other failure concerns.

Note that, if a probabilistic risk assessment (PRA) is available, it may help in establishing bounding levels for the needed reliability and for assessing the significance of software failures relative to other failures addressed in the PRA. In this example, suppose that a PRA has been performed and, based on the existing system prior to the digital upgrade, it used an overall probability P for failure of this particular trip function. Although an accurate value for the probability of a software common cause failure causing a failure to trip on demand cannot be established with present methods, the licensee concludes that the probability of such a failure would be much less than P (say an order of magnitude less) based on the evaluation of the software and its operating experience described above. The probability of a failure to trip would be dominated by other failure causes already accounted for (e.g., hardware failures, sensors, etc.). The analysis concludes that failures of this trip function caused by software are not a significant contributor to plant risk, based on the existing PRA.

The probability of the potential failure under consideration should be combined with the probabilities of other failures or events that also need to occur for the consequences of the failure to be significant. For example, if the system under review is a backup system that performs only when certain events occur, then a failure in that system may be important only if it occurs coincident with other events producing the need for the backup system. Failures may also be significant if they are not annunciated to the operator, thus reducing the possibility of timely repair. It is important to assess the combined probabilities to place the failure in the appropriate context and determine whether it is significant. This is illustrated in Example 5-4.

***Example 5-4. Combining Probabilities to Assess Significance of Potential Failures***

Consider an upgrade to the governors used on the emergency diesel generators. The existing analog electronic governors are to be replaced with new digital, microprocessor-based governors designed to perform the same function – controlling generator speed, and thus frequency. The governors on all of the redundant diesel generators would be replaced during an outage. Mechanical governors, which normally function as actuators for the electronic governors, also are currently installed and provide backup control of generator speed for certain failures of the electronic governor. The failure analysis identifies several potential system-level failures, including failure of the generator to come up to speed in an emergency start, and failure to control speed or frequency after the generator has started and loaded, causing loss of the generator. Errors in the software or firmware of the digital electronic governor are considered as one of a number of possible contributors to the overall likelihood of these system-level failures. The software was developed commercially and dedicated as part of the overall commercial dedication of the new governor for use on the diesel generators, using methods described in EPRI TR-106439. The development process was examined and information obtained on both the structure and complexity of the software, and on the operating history with the governing system including software. Based on this information, the licensee concludes that the system dependability is adequate and the likelihood of software failure occurring in multiple diesel generator governors is low relative to the likelihood of a hardware failure. Further, it is determined that for such a common cause software failure to be significant it must occur concurrently with

- Occurrence of an event that produces an actual need for emergency power to maintain plant safety (e.g., loss of coolant accident coincident with loss of offsite power), and
- Failure of the backup mechanical governors to take over speed control, and
- Failure of the plant operators to detect or to correct the problem with the governors (e.g., operators dispatched to the diesel generators to reset or restart the diesels, make a manual switchover to the backup mechanical governors, etc.).

Based on the dependability of the system combined with the low probabilities of these other events, the licensee concludes that software common cause failures in the new governors would not a significant concern. The 10 CFR 50.59 evaluation concludes there are no malfunctions with different results and no more than a minimal increase in the likelihood of malfunctions, and the change may be implemented under 10 CFR 50.59.

### *5.1.4 Identification of Appropriate Resolutions for Identified Failures*

Determining the appropriate resolutions for identified potential failures may include the following:

- No action – the failure does not pose significant risk and does not warrant any further consideration, as illustrated in Figure 3-2. This may be based on the assessment of likelihood of the failure per Section 5.3, and a comparison to other contributors to risk. Engineering judgment is typically involved in making these assessments. Results of Probabilistic Risk Assessments (PRAs) may also help in this process and provide a context in which to judge the particular failure being considered among all the other acknowledged contributors to risk in the plant.
- Modify the design or apply greater emphasis to appropriate parts of the design process to address the potential failure. If the failure is considered significant because of a lack of confidence (or difficulty in achieving reasonable assurance) in a portion of the design or in a particular software element in the design, then one option may be to apply additional design verification or testing activities. This additional design verification or testing could develop

the needed confidence and achieve reasonable assurance that the likelihood of the failure is such that it is no longer considered a significant risk. Alternatively, the design itself may be modified to either preclude the failure (e.g., make it fail safe for this particular failure) or add internal backups in the design, such as redundancy or diversity.

- Rely on existing backup capability offered by existing systems to address the failure – other equipment or systems that provide alternate ways of accomplishing the function or otherwise provide backup for this failure. This may include operator action if there is adequate information and time available for the operator to act, and with appropriate procedures and/or training.
- Supplement the existing backup capability such that the failure is adequately addressed. This could include improving the ability to detect the failure automatically so the repair response will be timely, improving procedures and training for the operators to mitigate the effects of the failure, or providing additional backup capability (e.g., manually operated switches for critical functions and procedural guidance for their use), so that the resulting risk is insignificant.

For any potential failure that poses a significant risk, there should be a means to annunciate the failure to the operator, so the fault can be repaired promptly.

Example 5-5 discusses the failure analysis for replacement of a simple, proven instrument such as a meter or transmitter. Example 5-6 shows how a failure analysis for a relatively complex system can identify a new failure that would lead to the need for a license amendment, and it illustrates some of the options available to the licensee for addressing this concern.

*Example 5-5. Failure Analysis for a Simple Meter Replacement*

Consider an upgrade in which an analog indicating device or meter is to be replaced with a microprocessor-based device. The function of the meter is to indicate to the control room operators the value of a single variable (e.g., pressure, temperature, flow, or level). In this case, the failure analysis is straightforward. There is a limited set of failure modes for the device (e.g., blank front panel, fail high, fail low, fail as-is) and these are sufficiently similar to those for the analog instrument. It is a widely used device with extensive operating history, and its failure rates are equal to or better than those of the analog device.

In cases where two of these devices would be used to provide redundant indication for a variable (e.g., Category 1 post-accident monitoring instruments), postulated common cause failures of the indicators caused by hardware or software are considered. The consideration takes into account that the instrument loops are qualified, independent, and separated, that the software utilized is small in scope and simple, that the operating history shows the device to be highly reliable, and that there are alternate indications for the variables available in the control room.

Based on the results of the failure analysis, the simplicity of the instruments and the low likelihood of failure, the licensee concludes that a license amendment is not required and the change can be implemented under 10 CFR 50.59. The important results of the failure analysis are documented, as is the 10 CFR 50.59 evaluation.

*Example 5-6. Failure Analysis for a Complex System*

In this example, a large portion of the Engineered Safety Features Actuation System (ESFAS) is to be replaced because the existing equipment used for signal conditioning and logic functions is obsolete and spare parts are difficult to obtain. A new system design has been developed that uses computer-based multiplexers to provide many of the input signals to the ESFAS, and microprocessors to implement logic and timing functions. The same microprocessors and software modules would be used in each channel of the new ESFAS design. Each multiplexer has multiple inputs and the ESFAS logic has multiple, individual outputs that together perform the safety-related functions, including the emergency core cooling function.

A failure analysis is performed early in the design process to identify any potential vulnerabilities in the design and to support licensing activities for the modification. It is noted that the system includes self-test features and associated diagnostics, but because of the large number of inputs and outputs and the functions that are being performed, it is difficult to demonstrate that a failure in the software or in a processor (e.g., processor lock-up) would always lead to a fail-safe configuration of the system outputs. Because the system has many inputs and outputs, extensive testing would be needed to demonstrate adequate protection against such failures, and this is not considered practical. The preliminary failure analysis concludes that potential failure modes include an unanalyzed configuration of ESF equipment (i.e., a combination of failure modes of the output states resulting in an ESF equipment configuration that has not been considered previously). The licensee determines that the effects of this type of failure on the system and the resulting impact on the plant have not been previously analyzed, and this would represent a malfunction with different results.

At this point the licensee considers a number of options available for addressing the concern. One is to analyze the effects of this type of failure in the Chapter 15 safety analysis and submit a proposed license amendment to NRC for review and approval prior to implementing the modification. Another option is to modify the design or make use of an alternate designs whose architecture, modularity or greater simplicity is such that there is reasonable assurance that the likelihood of the failure is less than those failures previously evaluated in the UFSAR. Failure management capabilities might be used to detect and annunciate failures, or prevent the unwanted output states from occurring. If this option is chosen, a failure analysis would be performed for the revised design and a 10 CFR 50.59 evaluation made to determine whether the new design would create any malfunctions with different results.

## 5.2 Defense In Depth and Diversity Analysis

A fundamental concept in the regulatory requirements and expectations for instrumentation and control systems in nuclear power plants is the use of four echelons of defense in depth:

- Control systems
- Reactor Trip System (RTS) and Anticipated Transient without Scram (ATWS)
- Engineered Safety Features Actuation System (ESFAS), and
- Monitoring and indications.

The control systems are designed to maintain the plant within normal operating conditions. In the event of excursions from these conditions, the reactor protection systems (RTS and ATWS) are designed to reduce reactivity and shut down the reactor. The engineered safety features actuation system (ESFAS) initiates mitigating functions to prevent release of radioactivity. Indications and controls in the control room allow operators to monitor the status of the plant and respond to plant events.

For substantial upgrades to trip logic or actuation portions of RTS or ESFAS, the potential consequences of a common cause failure due to software defects are likely significant enough (e.g., preventing all redundant protection channels from functioning) to warrant special treatment of the design. Specifically, the NRC expects that an analysis will be performed to assess the vulnerability to common cause failure and demonstrate that adequate diversity and defense-in-depth are available in the overall plant design to cope with such failure. The analysis is performed as part of the modification process, as shown in Figure 3-1.

The NRC's expectations for defense-in-depth and diversity analyses are described in BTP/HICB-19. The analysis is expected to determine whether safety functions are vulnerable to common cause failure, and if so, to identify diverse manual or automatic means that can perform the same or different functions in order to mitigate design basis accidents and transients. The acceptance criteria in BTP/HICB-19 are less restrictive than the plant design criteria in 10 CFR 50 (e.g., the ECCS design criteria in 10 CFR 50.46). Also, re-analysis of design basis events is permitted using "best estimate" conditions with realistic assumptions, rather than the more conservative design basis conditions required in 10 CFR 50, Appendix K. Consequently, the events analyzed per BTP/HICB-19 are considered "beyond design basis" events.

While the BTP/HICB-19 analysis is "beyond design basis," the results of the analysis feed into the design and licensing process (including the failure analysis) because they may identify additional diverse functions that should be added to the system being modified or to other plant systems. Satisfactory compliance with BTP/HICB-19 indicates that the potential consequences of common cause failure have been reduced to a level that presents acceptable risk. Failure to satisfy the BTP/HICB-19 acceptance criteria may indicate that further design changes are needed to better cope with potential common cause failure.

### 5.2.1 Applicability of Defense-in-Depth and Diversity Requirements

A formal defense-in-depth and diversity analysis per BTP/HICB-19 is expected only for substantial digital replacements of RTS and ESFAS as specified in BTP/HICB-19 and Section 7.0-A (e.g., Section C.1, Item 3) of the Standard Review Plan (see Figure 5-1). When in doubt as to whether a system is part of ESFAS, the UFSAR should be reviewed to determine how the system is described (e.g., described as part of ESFAS in Section 7.3 of Chapter 7 or as an auxiliary system per Chapter 9). The definitions of RTS and ESFAS in IEEE-603 (e.g., Figure 3 of IEEE 603) may also help. Since BTP/HICB-19 requires that the analysis be performed for each of the accidents and events in the UFSAR Chapter 15 safety analysis, only the trips (in RTS) or actions (in ESFAS) credited in the Chapter 15 safety analysis are evaluated in the defense-in-depth and diversity analysis.

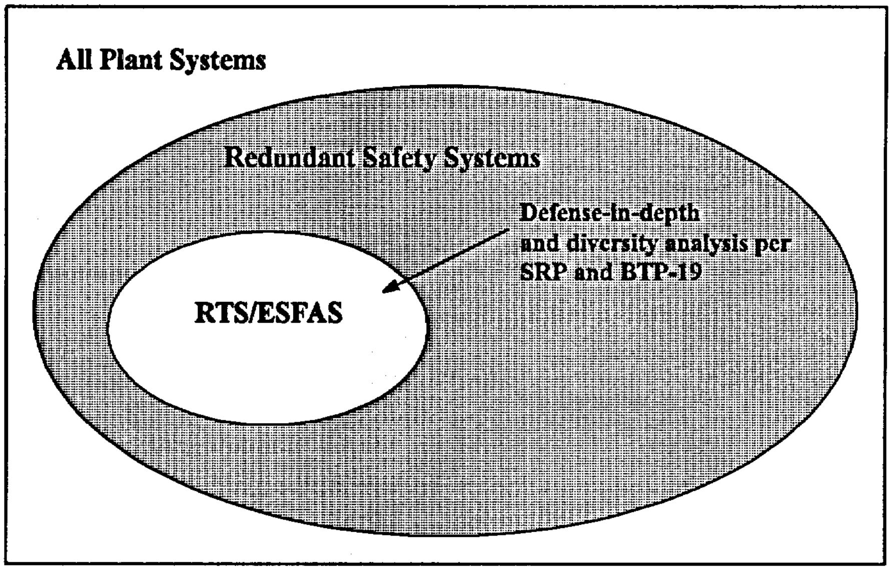



**Figure 5-2**
**Applicability of Defense-in-Depth and Diversity Requirements**

Consider, for example, the replacement of single loop controllers for both trains of Essential Service Water (ESW) system flow control. The system is initiated based on several Engineered Safety Features signals generated by the ESFAS system. However, while the ESW system is considered an Engineered Safety Features system, it is not part of the Engineered Safety Features *Actuation* System. Therefore, a formal defense-in-depth and diversity analysis per BTP/HICB-19 is not necessary.

Typically, the defense-in-depth and diversity analysis is performed when the trip logic and actuation portions of the RTS and/or ESFAS systems are upgraded with digital equipment. The analysis may or may not be required for digital component upgrades, such as for upstream instrumentation and sensors. For example, an analysis would not be required if there is reasonable assurance that the likelihood of software common cause failure is no greater than the likelihood of common cause failure of the existing analog hardware (or other hardware in the same system(s)) due to design flaws. When performed, the analysis may be very simple if the digital upgrade is not implemented at a level that impacts the defense-in-depth of the plant.

The cumulative effects of a series of upgrades or modifications should also be considered in the determination of whether a defense-in-depth and diversity analysis is performed. For any change to the plant, consideration should be given to the effects the change may have on diversity and defense-in-depth for RTS/ESFAS functions. If the change would affect the diversity and defense-in-depth of the RTS/ESFAS functions, then the analysis should be performed.

Also, if other I&C systems, including ATWS and other non-safety systems, are being upgraded to digital in plants where digital upgrades to RTS and/or ESFAS have already been done, prior defense-in-depth and diversity analyses should be reviewed. If the I&C system under consideration was credited in the prior analysis as providing backup, then the replacement digital equipment should be diverse from that used in the protection systems. NUREG-6303 provides guidance on methods that can be used to assess the diversity of digital systems.

### 5.2.2 Defense-in-Depth and Diversity Analysis Methods

While BTP/HICB-19 allows for re-analysis of postulated events, such analyses are costly and may not be necessary for upgrades to existing plants. For example, several defense-in-depth and diversity analyses for RTS upgrades at existing plants have used a methodology similar to the following:

- Identify system functions required for protection (RTS) or accident mitigation (ESFAS).
- Evaluate accidents to identify those that depend on the system protection/mitigating functions. Categorize accidents (not affected, system is backup for another system, system is primary but has automatic backup, system is primary and has manual backup).
- If the system is required to provide primary protection or mitigation, determine what happens if the required functions do not operate as a result of the postulated common mode failure.
- Determine what existing systems provide diverse automatic backup for the function (e.g., neutron instrumentation, core exit thermocouples, ATWS, etc.). Identify diverse indications that provide the operator with relevant plant status information. As noted by BTP/HICB-19, the diverse backup may be non-safety related, if it is of sufficient quality to perform the necessary function during the given event conditions.
- When diverse automatic action is not available, describe diverse indications and controls (including non-safety) that are present in the control room that allow the operator to perform the function. (Make sure these operator actions are covered by procedures and training.)
- In cases where the plant response results in a scenario that <u>is not bounded</u> by the existing analysis, determine whether there is an engineering rationale justifying that the BTP/HICB-19 acceptance criteria will be met. For example, if manual operator action takes longer than the primary automatic action, determine if the longer response time is acceptable based on best-estimate, realistic conditions.

Example 5-7 discusses the approach for the defense-in-depth and diversity analysis for the PLC-based load sequences upgrade discussed in Examples 4-6 and 4-8.

### 5.2.3 Diversity Required by the ATWS Rule

The regulation 10 CFR 50.62, which addresses mitigation of anticipated transient without scram (ATWS) events, requires equipment that is diverse from the reactor trip system, from sensor output to the final actuation device. When considering digital upgrades to the reactor protection system or to equipment installed under 10 CFR 50.62, the licensee should ensure that adequate diversity is maintained in accordance with the regulation. NUREG-6303 provides guidance for the evaluation of diversity.

Simple components or modules that are widely used and have extensive operational history (e.g., standard analog-to-digital converters, other standard or commodity type items) may be present in both systems and not compromise diversity. Determinations such as these should be documented. Note that these considerations also can be applied in assessing diversity used for defense-in-depth.

*Example 5-7. Defense-In-Depth and Diversity Analysis for Load Sequencer*

As part of the design of the PLC-based load sequencer upgrade discussed in Examples 4-6 and 4-8, the need to perform a defense-in-depth and diversity analysis was considered. Since the load sequencer is an integral part of the ESFAS system as described in Chapter 7.3 of the UFSAR, it was concluded that such an analysis should be performed in accordance with BTP HICB 19.

This analysis showed that in the unlikely event of a common mode failure of both sequencers in conjunction with certain design basis accidents, some required ESF equipment would not start automatically, which would generate alarms in the control room. Consequently, several new manual switches were added to the load sequencer panel to allow operators to manually start equipment. Since the "front-end" of the ESFAS system would still be functional, operators would be aware that ESF actuation signals had been generated but equipment had not started. The analysis showed that sufficient time would be available to manually start the equipment and comply with the BTP/HICB-19 acceptance criteria. The addition of the new manual switches was considered as part of the overall change in the 10 CFR 50.59 evaluation.

## 5.3 Assessing Digital System Dependability

This section provides additional guidance on addressing the issues associated with digital upgrades to ensure a high level of dependability. This guidance is intended to be used both in the design of digital upgrades and in engineering evaluations to support the 10 CFR 50.59 process. The ability to provide reasonable assurance that the digital upgrade will exhibit sufficient dependability is a key element of 10 CFR 50.59 evaluations as discussed in Section 4.

### *5.3.1 Factors that Affect Dependability*

As described in SECY 91-292 regarding NRC review of advanced light water reactor (ALWR) designs, digital I&C systems employ a greater degree of sharing of data transmission, functions, and process equipment as compared to analog systems. While this sharing enables some of the key benefits of digital equipment, it also increases the potential consequences of individual failures. Additionally, failures of digital equipment can be caused by latent software programming errors, which may not always be detected in design and testing of the system. Software defects can create common cause failures that can defeat the high dependability achieved by use of redundant safety system channels or non-diverse uses of the same software in other systems. The likelihood of software defects is minimized by the quality of the design process and the expertise of the software staff.

To support the licensing and 10 CFR 50.59 process, methods are needed to evaluate digital system quality and the likelihood of failure. For hardware, methods are well established for estimating reliability or probability of hardware failure. However, for software there are no well-established, accepted quantitative methods that can be used to estimate reliability, particularly for the high levels of reliability required of safety-critical software. Without such methods, other means must be used to gain reasonable assurance that the quality of the design is adequate. The answer lies in evaluation of the process used to develop the software, and characteristics of the resulting design. Although accepted methods for estimating software reliability are not presently available, there are well-established methods and engineering processes for development, evaluation, and control of software that can be used to produce highly dependable, high-quality digital systems.

In this guideline, the term *dependability* is used in relation to quality and likelihood of failures. This term reflects the fact that reasonable assurance of adequate quality and low likelihood of failure is derived from a qualitative assessment of the design process and the system design features. The term *dependability* also reflects the importance of ensuring that the system performs its functions in a consistent and repeatable manner and its behavior is predictable. A *reliable* system that performs its intended function, but exhibits other undesirable behavior, is not *dependable*.

To determine whether a digital system is sufficiently dependable, and therefore that the likelihood of failure is sufficiently low, there are some important characteristics that should be evaluated. These characteristics, discussed in more detail in the following sections, include:

- The development and quality assurance processes implemented for both the digital platform and the plant-specific application software (see Section 5.3.3). Compliance with appropriate industry standards and regulatory guidelines for development, software safety analysis, V&V, and configuration control should be demonstrated.
- Hardware and software design features that contribute to high dependability (see Section 5.3.4). Such features include built-in fault detection and failure management schemes, internal redundancy and diagnostics, and use of software and hardware architectures designed to minimize failure consequences and facilitate problem diagnosis.

The safety significance and simplicity of the system also play a role in assurance of quality and dependability (see Section 5.3.2). Software development activities need to be more rigorous for applications that have high safety significance. Systems that are sufficiently simple have more well-defined failure modes and tend to allow for more thorough testing of all input and output combinations than complex systems; complexity increases the uncertainty associated with demonstrating software quality.

In addition, the maturity of the product and in-service experience with the platform and the plant system application should be considered. Substantial applicable operating history reduces uncertainty in demonstrating adequate dependability. Credit should also be taken for using digital platforms that have previously been reviewed by the NRC as part of generic qualification for safety-related applications.

The final determination of dependability and likelihood of failures should consider the aggregate of all the factors described above. Some of these factors may compensate for weaknesses in other areas. For example, for a digital device that is simple and highly testable, thorough testing may provide additional assurance of dependability that helps compensate for a lack of operating history.

Even when appropriate design processes are followed in developing software and digital systems, because of the lack of well-established methods for estimating reliability or dependability, there still is some residual uncertainty when evaluating the potential for software errors to defeat safety functions in redundant, safety-related channels or result in faults in non-diverse uses of the same software (whether safety or non-safety related). Consequently, for certain safety system upgrades, the NRC expects that a formal analysis will be performed to demonstrate that adequate defense-in-depth and diversity is provided to cope with postulated accidents in the presence of common cause failures. Guidance on defense-in-depth and diversity analysis is provided in Section 5.2.

### 5.3.2 Safety Significance and Complexity

10 CFR 50, Appendix B, states that a quality assurance program will control activities "...affecting the quality of structures, systems, and components to an extent consistent with their importance to safety." Consequently, the rigor associated with the design, analysis, implementation, and quality assurance activities applied to digital upgrades should be commensurate with the safety significance of the system being modified.

Current standards and regulatory review guidance for digital equipment in nuclear power plants allow for gradations in design and verification activities on the basis of the safety significance and complexity of the system. The NRC has recognized that these are useful attributes on which to base decisions regarding the evaluation of digital systems. For example, Section C.2 in Appendix 7.0-A of the Standard Review Plan (NUREG-0800) states, in regard to software reviews, that "...the complexity and depth of the review can vary substantially depending upon the extent, complexity, and safety significance of the systems involved." Other digital upgrade activities including verification and validation, commercial item dedication, and defense-in-depth and diversity analysis include elements of safety significance and complexity.

EPRI TR-106439 notes that nuclear 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." The nuclear safety significance of a digital device should take into account the impact of failure of the digital device, which can be based on the results of the failure analysis or Probabilistic Risk Assessment (PRA) analyses.

If the device is used in a system that is not modeled in the PRA, then this may imply low nuclear safety significance, as long as it was explicitly screened out as not important to Core Damage Frequency (CDF) when the PRA was developed. Or, if the system is modeled, but the PRA shows this system has negligible effect on CDF (e.g., the system's probability of failure can be set to 0 or 1 with little change in CDF), then it may be concluded the system and thus the component is of low nuclear safety significance.

EPRI TR-106439 suggests that complexity be evaluated by considering the overall architecture of the component, device, or system; the number of functions; inputs and outputs; internal communications and multiple processors; interfaces with other systems or devices; and software characteristics (particularly branching and complexity of processing). The complexity of a system or device is not always obvious, but is an important characteristic to evaluate as an input to the determination of whether reasonable assurance can be achieved that the likelihood of failure is low.

Function point analyses or other measures of complexity being developed by the computer science community could be considered, but the NRC has not accepted any of these methods for use. IEC 61508 describes another approach for defining low complexity. Specifically, a low complexity system is considered to be one in which the potential failure modes of individual components are well defined and the behavior of the system under fault conditions can be determined.

### 5.3.3 Digital System Quality

The design of digital upgrades should place a high importance on quality and dependability. For digital equipment incorporating software, it is well recognized that prerequisites for quality and dependability are experienced software engineering professionals combined with well-defined processes for project management, software design, development, implementation, verification, validation, software safety analysis, change control, and configuration control.

For example, the NRC states in Appendix 7.0-A of the Standard Review Plan that "the review of design qualification for digital systems focuses, to a large extent, upon confirming that the applicant/licensee employed a high-quality development process that incorporated disciplined specification and implementation of design requirements. Inspection and testing is used to verify correct implementation and to validate desired functionality of the final product, but confidence that isolated, discontinuous point failures will not occur derives from the discipline of the development process."

IEEE 7-4.3.2-1993, endorsed by the NRC in Revision 1 of Regulatory Guide 1.152, provides guidance on important elements of the development process. Various other industry standards have also been developed to provide more detailed guidance on other aspects of software processes, and many of these have been endorsed by the NRC, as shown in Table 5-1.

In addition to the standards shown in Table 6-1, the following standards also can be used for guidance on development process issues:

- NUREG/CR-6294, Design Factors for Safety Critical Software
- ASME NQA-1, Subpart 2.7, Quality Assurance Requirements for Computer Software for Nuclear Facility Applications
- ANSI/IEEE 730, IEEE Standard for Software Quality Assurance Plans
- ANSI/IEEE 1016, IEEE Recommended Practice for Software Design Descriptions
- ANSI/IEEE 1063, IEEE Standard for Software User Documentation
- IEEE 1228, Standard for Software Safety Plans
- IEC 60880, Software for Computers in the Safety Systems of Nuclear Power Stations

**Table 5-1**
**Industry Software Standards Endorsed by NRC Regulatory Guides**

| Regulatory Guide | Endorsed Standard(s) | Scope of Requirements |
|---|---|---|
| RG 1.152, Rev. 1, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants" | IEEE Std 7-4.3.2-1993, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations" | Requirements to achieve high functional reliability and design quality for computers used as components of a safety system |
| RG 1.153, Rev. 1, "Criteria for Safety Systems" | IEEE Std. 603-1991, "Criteria for Safety Systems for Nuclear Power Generating Stations" | Minimum functional and design requirements for the power, instrumentation, and control portions of safety systems |
| RG 1.168, "Verification, Validation, Reviews, And Audits For Digital Computer Software Used in Safety Systems of Nuclear Power Plants" | IEEE Std 1012-1986, "IEEE Standard for Software Verification and Validation Plans" * | Elements of software V&V plans and minimum V&V activities to be included in the plan |
| | IEEE Std 1028-1988, "IEEE Standard for Software Reviews and Audits" * | Guidance on conducting audits, inspections and walkthroughs, and technical and management reviews |
| RG 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" | IEEE Std 828-1990, "IEEE Standard for Software Configuration Management Plans" * | Guidance on an approach to planning configuration management for safety system software |
| | IEEE Std 1042-1987, "IEEE Guide to Software Configuration Management" | Guidance for implementing software configuration management plans developed per IEEE-828 |
| RG 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" | IEEE Std 829-1983, "IEEE Standard for Software Test Documentation" * | Method for software test documentation, including test planning, test specification, and test reporting |
| RG 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" | IEEE Std 1008-1987, "IEEE Standard for Software Unit Testing" | Guidance on unit testing of software as part of an overall software V&V plan |
| RG 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" | IEEE Std 830-1993, "IEEE Recommended Practice for Software Requirements Specifications" * | Guidance on development of software requirements specifications |
| RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" | IEEE Std 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes" * | Describes processes and activities that compose a software development process |

* These standards have been superseded. As of the date of this guideline, the NRC has not formally endorsed the more recent versions.

#### 5.3.3.1 Software Life Cycle and Development Process

A fundamental concept of quality assurance for software is that the development and use of software should follow a defined life cycle in order to minimize errors in design and in use. The software life cycle is a progression of stages in which specific design activities are performed, design outputs are generated, evaluations such as software safety analysis are performed, verification and validation is performed (e.g., checks, reviews, and/or tests), the configuration of the digital system is controlled, and errors uncovered in previous phases are corrected. Section 3 describes the relationship of these activities to the typical plant design change process.

Standards, methods, and guidelines are available that allow the licensee and the vendor to assure adequate design quality through design, software safety analysis, verification, validation, configuration control, and change control. Guidance for computer software development for safety systems is provided in IEEE 7-4.3.2. Compliance with IEEE 7-4.3.2 requires that software be developed in accordance with a software quality assurance plan that is consistent with the requirements of ASME NQA-2a, Part 2.7 (which is now contained in Part II of ASME NQA-1). Additional guidance on software life cycle processes is provided in IEEE 1074, which is endorsed by Regulatory Guide 1.173.

In implementing a digital system, the licensee should evaluate the life cycle process used by the digital system vendor and any third parties involved in system integration or application development. The licensee should also establish its own life cycle process for the operation and maintenance of the system in their plant.

Regulatory review guidance for digital systems contained in Appendix 7.0-A of the NRC's Standard Review Plan (NUREG-0800) places a large emphasis on the software life cycle and development process. Detailed expectations related to software development are described in Branch Technical Position (BTP)/HICB-14, "Guidance on Software Reviews for Digital Computer Based Instrumentation and Control Systems," which is included in Chapter 7 of NUREG-0800. The fundamental expectations of BTP/HICB-14 are that (1) acceptable plans are prepared to control software development activities, (2) the plans are followed in an acceptable software life cycle, and (3) the process produces acceptable design outputs.

#### 5.3.3.2 Types of Software in Digital Systems

It is important to note that there are several different types of software that may be involved in a digital system, potentially with different organizations responsible for each, including:

- **Base software** previously developed by a vendor under their own development process and delivered with the system, often as embedded firmware.
- **Application-specific software** including custom programs such as ladder logic implemented on a PLC.
- **Configuration data** including settings that define the specific configuration (such as I/O point assignments, communication addresses, etc.) for a digital based system as well as values which define the plant-specific characteristics of a system (I/O point engineering units, limits, setpoints, etc.).

- **Software tools for testing, calibration, or configuration** of the digital system, such as software provided by the vendor to assist in loading, documenting, and verifying the application program or configuration data. Unlike the other categories above, this software is typically not used on-line (at run time) in the system.

The duties for software development and quality assurance for the different types of software used should be clearly specified. For a safety-related system, application software and configuration data is generated and controlled under a 10 CFR 50, Appendix B, quality assurance program.

#### 5.3.3.3 Software Verification and Validation

Software verification and validation (V&V) is a series of activities intended to detect errors and defects as early in the development as possible (when they are most easily corrected), and once detected, to ensure they are appropriately resolved. Software *verification* consists of reviews performed on the outputs from each phase of development to ensure that requirements are met and unintended functions are not created. Software *validation* is typically testing of actual software (or portions of software) to demonstrate that the software properly implements the requirements, under various conditions, without unintended functions. These activities are expected to be performed in accordance with a defined plan that describes the V&V activities, responsibilities, and documentation for each phase of the life cycle. More detailed definitions of software verification and validation are provided in the relevant industry standards, including IEEE 7-4.3.2 and IEEE 1012. EPRI has also developed a handbook, TR-103291, providing guidance on V&V planning and methods.

Another expectation regarding V&V is that personnel performing V&V tasks are independent of those responsible for developing the software. Independence of V&V activities may increase the odds of finding a problem and dispositioning it properly. Regulatory Guide 1.168 states that "...this independence must be sufficient to ensure that the V&V process is not compromised by schedule and resource demands placed on the design process."

The level of independence and types of V&V activities applied for safety system software should be commensurate with the importance of the digital system to plant safety, availability, and investment protection; the complexity of the system and the associated software; and the degree of reliance on the software (e.g., the degree to which there are backups available for the functions provided by the software). The results of the failure analysis described in Section 5.1 assist in making this determination. Guidance on use of safety significance to define appropriate V&V activities is provided in IEEE 1012, particularly in the 1998 revision.

#### 5.3.3.4 Software Configuration and Change Management

Because configuration and change control is a life cycle activity, the licensee needs to implement a method for carrying out this responsibility over the service life of the equipment. Guidance on development of configuration management plans is provided in IEEE 828, which is endorsed by Regulatory Guide 1.169.

Experience has shown that significant errors can result from making changes to software or improperly controlling those changes. Evaluating the effects of changes to one software element on the performance of a system that may include many other software elements is therefore very important. Tests to verify that changes do not adversely affect the rest of the system and are compatible with previously released hardware and software are referred to as "regression" tests.

#### 5.3.3.5 Software Safety Analysis

The NRC has recognized that an important element of developing quality software is a process of identifying and analyzing potential hazards that can affect the safety of the system and the plant. Such hazards may result either from failures or unanticipated behavior of the digital system, or from external conditions or events. Regulatory review guidance in BTP/HICB-14 and in Regulatory Guide 1.173 states that there should be a defined safety analysis process in which responsibilities and activities are defined for each phase of the development process.

This process is similar to the V&V process, which is intended to ensure that defined requirements are carried through into the final implementation of the system, except that the safety analysis process focuses on identifying requirements that are needed in order to prevent or mitigate hazards. As in the V&V process, it is appropriate to employ a graded approach based on the safety significance of the plant system. Guidance for software safety analysis activities is contained in IEEE Standard 1228. The software safety analysis concept is consistent with the failure analysis guidance given in Section 5.1.

#### 5.3.3.6 Use of Commercial Off the Shelf (COTS) Equipment

The availability of replacement I&C equipment developed under a 10 CFR 50 Appendix B program is severely limited. As a result, the ability to use commercially developed "off-the-shelf" equipment, properly qualified for use in nuclear plant systems, is critical to continued safe and economic operation of existing nuclear power plants. Also, commercial equipment that has an extensive operating history in other similar applications may, when properly applied, provide greater reliability and safety than equipment that is custom developed specifically for the application at hand.

However, commercial vendors of equipment containing software or firmware often have not completed a V&V program at the level of the requirements and standards discussed above. Thus, the licensee should ensure that appropriate activities are undertaken to develop an equivalent level of confidence in the commercial grade item's software as well as the hardware. This is done through design qualification and commercial grade item dedication.

Section 5.3.3.6 and Annex D of IEEE 7-4.3.2-1993 provide guidance on qualification of commercial grade digital equipment. EPRI TR-106439 provides additional guidance for the evaluation and acceptance of commercial grade digital equipment within the established commercial grade item dedication process. The NRC has endorsed TR-106439 and refers to the document in Chapter 7 of the Standard Review Plan (Appendix 7.0-A and BTP/HICB-14).

Integral to the process described in TR-106439 is use of a graded approach depending safety significance and complexity of the device and the plant application. A supplemental guideline, EPRI TR-107339, also provides useful information and is intended to provide "how to" guidance and examples.

### *5.3.4 Digital System Design and Performance*

For protection and safety systems in nuclear power plants, the minimum functional design criteria are specified in IEEE 603 and IEEE 279 (see 10 CFR 50.55a(h) for applicability). Note that plants which were licensed to IEEE 279, and plants licensed before IEEE 279, do not have to meet the requirements of the newer IEEE 603 standard (see 10 CFR 50.55a(h) for specific circumstances that may require upgrading to the newer standard). However, many vendors are now designing systems to meet IEEE 603, and compliance with IEEE 603 will also satisfy IEEE 279.

Additional design requirements specific to digital systems are specified in IEEE 7-4.3.2. These digital specific requirements cover the development process, as described above, and other aspects of digital system design that affect dependability and performance. This section summarizes some of the key design and performance issues that relate to the quality of digital equipment. These issues should be considered when identifying potential system vulnerabilities in the failure analysis.

EPRI 1001045 also provides a comprehensive discussion of design and implementation issues for digital systems. While its focus is primarily on application of digital platforms that have been qualified on a generic basis, its design guidance can be applied to any digital upgrade.

#### 5.3.4.1 Hardware Qualification

Equipment installed as part of an upgrade should be designed and installed to be compatible with its environment. In addition to environmental variables such as seismic accelerations, temperature, humidity, and radiation, this should include consideration of electromagnetic compatibility (EMC). Requirements for qualification of electronic equipment are specified in IEEE 323 (endorsed by Regulatory Guide 1.89), and extensive guidance on equipment qualification is provided in EPRI TR-100516, "Nuclear Power Plant Equipment Qualification Reference Manual." Draft Regulatory Guide DG-1077, "Guidelines for Environmental Qualification of Microprocessor-Based Equipment Important to Safety in Nuclear Power Plants," provides guidance on environmental qualification of digital equipment.

Regarding EMC qualification, EPRI TR-102323 and Regulatory Guide 1.180 provide guidance for addressing the EMC issue for digital upgrades. Qualification of equipment for electromagnetic compatibility requires demonstration that the levels of electromagnetic interference (EMI) that will be present in the installed environment are below the levels at which the equipment is susceptible. Equipment susceptibilities are typically determined through laboratory testing, and are often performed by the manufacturer. Comparison to the installed environment can be accomplished by (1) performing site surveys at the point of installation to show that the electromagnetic environment is acceptable for the equipment and its known susceptibilities, or (2) reliance on generic levels established by the industry for nuclear plant environments, coupled with compliance to certain limiting practices as described in TR-102323.

EMI emission levels from the equipment also should be shown to be acceptable for the planned environment. Again, equipment emission levels are typically determined by laboratory testing. EPRI TR-102323 provides acceptable generic emission levels for nuclear power plants.

Recent experience with generic qualification of digital equipment has shown that available digital equipment may not fully comply with all EMC levels specified in the industry guidelines. In cases where full compliance with accepted EMC levels has not been demonstrated, the licensee can take additional action to ensure acceptable performance of the equipment, including:

- Demonstrate that for the EMI/RFI levels at which the digital equipment is susceptible, there are no credible threats to the equipment as installed (e.g., via site surveys and/or analysis).
- Demonstrate that the types of behavior observed in the susceptibility testing will not adversely affect the safety function of the digital equipment. For example, short-term, high-frequency variations in the output of the device in response to EMI disturbances may not impact the safety-related function or adversely affect plant operation if the device continues to operate and the system can meet its safety-related performance requirements.
- Demonstrate that equipment in close proximity to the installed digital equipment will not be susceptible to emissions from the new equipment.
- Implement actions to mitigate unacceptable EMI/RFI emissions, such as adding a secondary enclosure, additional cable and wire shielding, or power line filtering or conditioning. Mitigating actions might also include administrative controls on EMI/RFI sources, such as handheld radios, cellular telephones, and radio repeaters.

#### 5.3.4.2 Human Factors

The human-system interface includes all points of interaction between the digital system and plant personnel, including:

- Operators – alarms, status displays, control interfaces, etc.
- Maintenance technicians – test and calibration interfaces, diagnostic information displays, data entry terminals for setpoints, configuration workstations or terminals, etc.
- Engineering personnel – configuration workstations or terminals, etc.

The principal concern related to the human-system interface is the possibility of system failure due to human error, or due to unauthorized entries or alterations of the system through a maintenance, test, or configuration interface. Adequate administrative controls, security, appropriate training, and plant procedures should be provided to minimize the possibility of such events. These types of potential failures should be considered in the failure analysis described in Section 5.1.

Human factors considerations should be addressed in the design of all human-system interfaces associated with the upgrade in order to minimize the possibility for human error. IEEE 603 discusses the application of human factors considerations in the design process for safety systems. Regulatory review guidance is provided in Chapter 18 of the Standard Review Plan (NUREG-0800) which also references NUREG-0700, "Human-System Design Review Guideline," and NUREG-0711, "Human Factors Engineering Program Review Model." EPRI 1001045 also provides guidance on human factors design considerations for digital upgrades.

Consideration should also be given to the effect the change would have on the Plant Simulator to support operator training, while meeting requirements for fidelity to the existing plant prior to the change. Consequently, for large digital upgrades, a separate mock-up facility may be needed to allow testing and training on the new equipment before it is installed while still enabling operators to maintain their qualifications with the existing equipment.

#### 5.3.4.3 System Integrity and Failure Management

The intrinsic complexity of digital devices, including both hardware (e.g., numerous I/O points, integrated circuits, and microprocessors) and software (e.g., communications, logic, and data bases) provides an opportunity for failures, abnormal conditions, or defects to cause unexpected behaviors. System integrity refers to the ability of the device to perform its function when subjected to adverse internal or external conditions. Failure management refers to the ability of the device to identify failures, and to alarm them. Section 5.5 of IEEE 7-4.3.2 describes system integrity requirements for digital systems.

Good system integrity and failure management will typically result if the design of the device includes consideration of plausible failures and defects and provides appropriate features to detect the results of such events. Per IEEE 7-4.3.2, digital equipment should be designed to continue to perform its design function in the presence of internal or external conditions that have significant potential to defeat the function. Diagnostic features should be used to alert the operations staff of failures, allowing for timely repair of faulted equipment. The use of duplex or triplex digital equipment (equipment with internal double or triple redundancy) within redundant protection channels should consider the guidance contained in Generic Letter 91-18, "Information to Licensees Regarding Two NRC Inspection Manual Sections on Resolution of Degraded and Non-Conforming Conditions and on Operability."

The NRC has recognized that internal diagnostics coupled with periodic surveillance tests should provide an adequate method for assuring that detectable failures or undesirable behavior can be identified. Regulatory review guidance on this topic is provided in BTP/HICB-17, "Guidance on Self-Test and Surveillance Test Provisions," in Chapter 7 of the Standard Review Plan (NUREG-0800). Depending on the extent of internal diagnostic and self-test features, plants may be able to use these capabilities to reduce requirements for manual surveillance testing and/or extend surveillance intervals.

### 5.3.4.4 Real-Time Performance

Data communications inside a digital device take time and have an impact on the response of the digital device. Also, sampling of input signals and conversion to digital representations can introduce errors (e.g., due to digital resolution or aliasing) if the digital device is not properly designed or applied. These real-time performance issues should be evaluated to ensure functional requirements are satisfied.

For example, in a protection system application, the response time of a digital device (which may vary depending on the physical configuration of the device and the computational requirements of the application program) should be evaluated to ensure there is sufficient time to sense a trip condition and actuate downstream equipment. If the processing time increases beyond that required for the analog device, safety limits may be affected. It is important to note that the sampled nature of digital devices requires that additional time be allowed beyond the basic system cycle time when determining the overall response time of the device.

Also important are the potential benefits that can be derived from the replacement of analog equipment with digital devices. In particular, digital devices often will provide improved accuracy due to elimination of drift and this can be used as a basis for changing safety system trip setpoints, which in turn provides increased thermal power margin.

Guidance on the subject of real-time performance is provided in NUREG-1709, "Selection of Sample Rate and Computer Word Length in Digital Instrumentation and Control Systems." Regulatory review guidance is provided in BTP/HICB-21, "Guidance on Digital Computer Real-Time Performance," in the Standard Review Plan (NUREG-0800).

### 5.3.4.5 Security Considerations

Security of digital systems should be provided so that access to configuration settings, software, and data is controlled and unauthorized changes are prevented. Specific requirements relating to system security are contained in industry standards such as IEEE 279 and IEEE 603. The NRC has also recognized the importance of security and access control in preserving the safety functions performed by software, and regulatory guidance on the subject is included in the Standard Review Plan for digital systems. As noted in Section 7.1-C of the SRP, access controls should address access via network connections, or via maintenance equipment. Additional guidance is provided in Section 7.9 of the SRP regarding access to safety systems through off-site connections. BTP/HICB-14 also includes review guidance pertaining to security in the software development process.

# 6
# REFERENCES


1. Code of Federal Regulations Title 10, Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants."

2. Code of Federal Regulations Title 10, Part 50.59, "Changes, Tests and Experiments."

3. Code of Federal Regulations Title 10, Part 50.62, "Requirements for Reduction of Risk from Anticipated Transients Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants."

4. Federal Register Notice, "Changes, Tests, and Experiments," Volume 64, Number 191, Pages 53582-53617, October 4, 1999.

5. NEI 96-07, Revision 1, "Guidelines for 10 CFR 50.59 Implementation," November 2000.

6. SECY 91-292, "Digital Computer Systems for Advanced LWR."

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

8. Generic Letter 91-18, "Information to Licensees Regarding Two NRC Inspection Manual Sections on Resolution of Degraded and Non-Conforming Conditions and on Operability."

9. NUREG-0700, "Human-System Interface Design Review Guideline," Revision 1, June 1996.

10. NUREG-0711, "Human Factors Engineering Program Review Model," July 1994.

11. NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, Chapter 7," Revision 4, June 1997.

12. NUREG-1709, "Selection of Sample Rate and Computer Wordlength in Digital Instrumentation and Control Systems," June 2000.

13. NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," December 1994.

14. NUREG/CR-6294, "Design Factors for Safety-Critical Software,"October, 1994.

15. Regulatory Guide 1.22, "Periodic Testing of Protection System Actuation Functions."

16. Regulatory Guide 1.152, Revision 1, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants."

17. Regulatory Guide 1.153, Revision 1, "Criteria for Safety Systems."

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

19. Regulatory Guide 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

20. Regulatory Guide 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

21. Regulatory Guide 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

22. Regulatory Guide 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

23. Regulatory Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

24. Regulatory Guide 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis."

25. Regulatory Guide 1.176, "An Approach for Plant-Specific Risk-Informed Decisionmaking: Graded Quality Assurance."

26. Regulatory Guide 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems."

27. Regulatory Guide 1.187, "Guidance for Implementation of 10 CFR 50.59, Changes, Tests, and Experiments."

28. Draft Regulatory Guide DG-1077, "Guidelines for Environmental Qualification of Microprocessor-Based Equipment Important to Safety in Nuclear Power Plants."

29. NSAC-105, "Guidelines for Design and Procedure Changes in Nuclear Power Plants."

30. EPRI NP-5652, "Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications."

31. EPRI TR-100516, "Nuclear Power Plant Equipment Qualification Reference Manual," January 1992.

32. EPRI TR-102323, "Guidelines for Electromagnetic Interference Testing in Power Plants," Revision 1, January 1997.

33. EPRI TR-102400, "Handbook for Electromagnetic Compatibility of Digital Equipment in Power Plants," October 1994.

34. EPRI TR-103291, "Handbook for Verification and Validation of Digital Systems," Revision 1, December 1998.

35. EPRI TR-104595, "Abnormal Conditions and Events for Instrumentation and Control Systems: Volume 1: Methodology for Nuclear Power Plant Digital Upgrades; Volume 2: Survey and Evaluation of Industry Practices," January 1996.

36. EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," October 1996.

37. EPRI TR-107339, "Evaluating Commercial Digital Equipment for High Integrity Applications: A Supplement to EPRI Report TR-106439," December 1997.

38. EPRI TR-108831, "Requirements Engineering for Digital Upgrades," December 1997.

39. EPRI 1001045, "Guideline on the Use of Pre-Qualified Digital Platforms for Safety and Non-Safety Applications in Nuclear Power Plants," December 2000.

40. NEI White Paper, "Standard Format for Operating License Amendment Requests from Commercial Reactor Licensees," March 15, 2001.

41. IEEE 279-1971 (withdrawn), "Criteria for Protection Systems for Nuclear Power Generating Stations."

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

43. ANSI/IEEE 730-1989, "IEEE Standard for Software Quality Assurance Plans."

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

45. IEEE 829-1983, "IEEE Standard for Software Test Documentation."

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

47. IEEE 1008-1987, "IEEE Standard for Software Unit Testing."

48. IEEE 1012-1998, "Standard for Software Verification and Validation."

49. ANSI/IEEE 1016, "IEEE Recommended Practice for Software Design Descriptions."

50. IEEE 1042-1987, "IEEE Guide to Software Configuration Management."

51. ANSI/IEEE 1063, "IEEE Standard for Software User Documentation."

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

53. IEEE 323-1983, "Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations."

54. IEEE 379-1994, "Standard Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems."

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

56. IEEE 7-4.3.2-1993, "Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations."

57. IEEE 1228-1994, "Software Safety Plans."

58. ASME NQA-1-1997, "Quality Assurance Requirements for Nuclear Facility Applications."

59. ASME NQA-2a-1990, "Quality Assurance Requirements for Nuclear Facility Applications."

60. IEC 60880, "Software for Computers in the Safety Systems of Nuclear Power Stations."

61. IEC 61508, "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems."

62. ISA-RP67.04.01-2000, "Methodologies for the Determination of Setpoints for Nuclear Safety-Related Instrumentation."

# A
# SUPPLEMENTAL QUESTIONS FOR ADDRESSING 10 CFR 50.59 EVALUATION CRITERIA

NEI 96-07, Revision 1, and Section 4 of this guideline provide a set of eight questions consistent with the criteria in 10 CFR 50.59(c) used to determine if a modification requires prior NRC review and approval. This appendix provides items to consider in answering each of these eight questions. These supplemental items are posed as questions with yes or no answers. It is important to keep in mind that an answer of "yes" or "no" to one of these supplemental questions does not automatically mean that the criteria of 10 CFR 50.59 have been met for changes that would require a LAR. Instead, these questions are merely intended to assist the user in identifying relevant issues for the 10 CFR 50.59 evaluation.

The supplemental questions provide a structure that may be included with the 10 CFR 50.59 evaluation to support and document the engineering judgement used to determine if the change can be implemented under 10 CFR 50.59. A simple "yes" or "no" answer provides no evidence of such judgement. The 10 CFR 50.59 questions should be answered in sufficient detail, either by reference to a source document or by direct statements, that an independent third party can verify the judgements.

Note that for a particular upgrade, some of the items listed may be more appropriately addressed in the evaluation of a different 10 CFR 50.59 question or in several of the questions. The items listed are intended to serve as a guide for the 10 CFR 50.59 evaluation and are not intended to be all-inclusive; there may be aspects of a digital upgrade that are not highlighted by this appendix that may result in the upgrade requiring prior NRC review and approval (via LAR).

**1. Does the activity result in more than a minimal increase in the frequency of occurrence of an accident?**

Areas that should be addressed in responding to this question include the following:

(a) Does the new equipment installed with the upgrade exhibit performance characteristics, or have design features, that give an increased frequency of a system malfunction resulting in an accident? The system failure analysis can help provide the answer to this question. The assessment of a change in frequency may be made on a qualitative basis, particularly for systems or components which rely on software because there does not currently exist a consensus method for quantifying software reliability. Section 5 of this document provides additional guidance on system failure analysis.

(b) Does the system exhibit performance characteristics that increase the need for operator intervention or increase operator burden to support operation of the system in normal or off-normal conditions? Could this increase the frequency of an accident previously evaluated?

(c) Is the system compatible with the installed environment (e.g., temperature, humidity, seismic, electromagnetic fields, airborne particulates) such that system performance will not be degraded compared to the system being replaced?

(d) Can the system have an adverse impact on the installed environment (e.g., temperature, humidity, seismic, EMI/RFI emissions, airborne particulates) such that performance of an existing system used for accident detection will be more than minimally degraded compared to existing requirements?

**2. Does the activity result in more than a minimal increase in the likelihood of occurrence of a malfunction of an SSC important to safety?**

Areas that should be addressed in responding to this question include the following:

(a) Does the modified system meet the required plant environmental and seismic envelopes?

(b) Could the environment in which the upgraded equipment operates cause an increase in the likelihood of failure (e.g., electromagnetic susceptibility in a higher frequency range)? Could the new system create an environment (e.g., temperature, humidity, seismic, EMI/RFI emissions, airborne particulates) which adversely affects other equipment and increases the probability of occurrence of a malfunction?

(c) Have potential interactions between safety-related and non-safety related systems been addressed?

(d) Are the electrical loads associated with the upgraded system addressed in the design?

(e) Does the plant HVAC have adequate capacity for the thermal loads of the upgraded system?

(f) Does the upgraded system meet applicable requirements for separation, independence, and grounding?

(g) Does the upgraded system have adequate cabinet cooling?

(h) Could a common cause failure result in a system-level failure based on the failure analysis (also see Item (i))?

(i) Is there reasonable assurance that the dependability of the system is sufficient (i.e. the likelihood of failure is significantly below that of single, active failures)? Was the application software developed under a 10 CFR 50 Appendix B, QA program using a documented life-cycle development process? Does the design comply with industry and regulatory standards? Is there prior operating history for the digital device(s) and their firmware? Has the platform been pre-qualified through NRC review? Does the design include features to detect, annunciate, and/or mitigate faults? Has the system been tested under all normal and abnormal operating conditions?

(j) Is there a clear trend toward increasing the likelihood of malfunction of the SSC(s)?

**3. Does the activity result in more than a minimal increase in the consequences of an accident?**

The following areas should be addressed in responding to this question to determine if the activity results in an increase in radiological releases above the licensing limit:

(a) Does the system directly contribute to accident prevention or mitigation? If so, could the system cause the consequences (i.e. radiological release) of the accident to increase more than minimally?

(b) Does the upgraded system exhibit a response time beyond current acceptance limits (e.g., because of sample period, increased filtering)?

(c) Does the system perform adequately under high duty cycle loading (e.g., computational burden during accident conditions)?

(d) Does the architecture of the system exhibit a single failure that results in more severe consequential effects (e.g., reduced segmentation due to combining previously separate functions, several input channels sharing an input board, central loop processor for many channels)? System failure analysis helps to answer this question.

(e) Does the human-system interface design introduce increased burdens or constraints on the operators' ability to adequately respond to an accident, for operator actions credited in the licensing basis, such that there are more severe consequential effects (e.g., inability to access and operate more than one control at a time)?

(f) Could the new system create an environment (e.g., temperature, humidity, seismic, EMI/RFI emissions, airborne particulates) which adversely affects other equipment used for accident mitigation such that the consequences of an accident are more than minimally increased?

**4. Does the activity result in more than a minimal increase in the consequences of a malfunction?**

Areas that should be addressed to determine if the activity could result in an increase in the radiological releases above the current licensing limit include the following:

(a) Does the system play a role in mitigating the consequences (i.e. radiological release) of a malfunction? If so, would the change result in more than a minimal increase in the consequences of the malfunction?

(b) Does the upgraded system exhibit the same failure modes affecting radiological releases as the system being replaced (e.g., fail low, fail high, fail-as-is, diagnostic failures)? If the failure mode is different, are the consequences increased beyond what was evaluated previously in the SAR?

(c) Is there a means available to alert the operators to the failure condition? Are the consequences bounded by other events evaluated in the SAR?

(d) Can the system have an adverse impact on the installed environment (e.g., temperature, humidity, seismic, EMI/RFI emissions, airborne particulates) such that performance of an existing system used for accident mitigation will be more than minimally degraded compared to existing requirements?

**5. Does the activity create a possibility for an accident of a different type?**

Areas that should be addressed in responding to this question include the following:

(a) Have the assessments of system-level failure modes and effects for the new system or equipment identified any new types of system-level failure modes that could cause a different type of accident than presented in the plant SAR?

(b) Plant SAR analyses were based on credible failure modes of the existing equipment. Does the replacement system change the basis for the most limiting scenario?

(c) Has power supply quality been considered (e.g., high harmonics from inverters, slow loss of voltage, or high voltage conditions)?

(d) Could the new system create an environment (e.g., temperature, humidity, seismic, EMI/RFI emissions, airborne particulates) which adversely affects other equipment and creates the possibility of an accident of a different type?

**6. Does the activity create a possibility for a malfunction of an SSC important to safety with a different result?**

These areas should be addressed in responding to the question:

(a) Does the change involve combining previously separate functions into one digital device such that a failure creates a result not bounded by the results of malfunctions previously considered in the UFSAR?

(b) Based on a qualitative assessment, is there reasonable assurance that failures due to software, including software common cause failures are unlikely (i.e. no more likely than other potential common cause failures such as maintenance or calibration errors that are not considered in the UFSAR)? If not, are the results of the software common cause failure different than (i.e. not bounded by) the results of the malfunctions considered in the UFSAR?

(c) Could the environment in which the upgraded equipment operates cause a new type of failure (e.g., electromagnetic susceptibility in a higher frequency range)? Could the new system create an environment (e.g., temperature, humidity, seismic, EMI/RFI emissions, airborne particulates) which adversely affects other equipment and thereby creates the possibility of a different type of malfunction?

(d) Does the upgraded system have the same failure mode on loss of power as the system being replaced? If the failure mode is different, are the consequences increased beyond what was evaluated previously in the SAR?

(e) Is the response of the upgraded system on restoration of power different from that of the system being replaced? If so, are the consequences bounded by what was evaluated previously in the SAR?

(f) Does the system or equipment reset to operating parameters and settings established for the specific system, or does it go to a default set of parameters when the system is reset? If the system is reset with factory default parameters, what effect do they have on plant operation? Are the consequences bounded by what was evaluated previously in the SAR?

(g) Does the human-system interface (HMI) introduce failure modes different from those of the existing system? If so, are the results bounded by what was evaluated previously in the SAR?

(h) Have assessments of system-level failure modes and effects for the new system or equipment identified any new types of system-level failures (that are as likely to occur as those failures previously considered in the UFSAR) that would result in effects not bounded by the results previously considered in the SAR?

**7. Does the activity result in a design basis limit for a fission product barrier being exceeded or altered?**

The areas to be addressed include the following:

(a) Are any of the numerical values in the UFSAR that are used directly in the determination of the integrity of the fission product barriers associated with the change? Would the digital upgrade result in any of these values being exceeded or altered?

(b) Has the digital upgrade decreased the channel trip accuracy beyond the acceptance limit?

(c) Has the digital upgrade increased the channel response and/or processing time beyond the acceptance limit?

(d) Has the digital upgrade decreased the channel indicated accuracy?

**8. Does the activity result in a departure from a method of evaluation described in the UFSAR used in establishing the design bases or in the safety analysis?**

The areas to be addressed include the following:

(a) Does the upgrade involve a change to any element of the analytical methods that are described in the UFSAR which are used to demonstrate the design meets the design basis or that the safety analysis is acceptable?

(b) Does the change involve use of a method of evaluation not already approved by the NRC?

# B

# OUTLINE FOR DOCUMENTING 10 CFR 50.59 SCREENS AND EVALUATIONS

## Introduction

10 CFR 50.59, paragraph (d) requires that records be maintained of the changes made to the facility that are evaluated against the eight criteria in paragraph (c)(2) of the section. NEI 96-07 clarifies that documentation of the 10 CFR 50.59 evaluation is required (and will be submitted to the NRC at least every 24 months) for changes implemented under the rule, however the rule does not require documentation of the screening evaluation.

This appendix is intended to provide a suggested outline that could be used to support the 10 CFR 50.59(d) documentation requirements for a digital upgrade. The outline could also be used to document the results of a screening evaluation for changes that screen out and do not require a 10 CFR 50.59 evaluation. It is intended to be used for information only and has not been endorsed by the NRC. The suggested outline is provided below, along with a brief description of the type of issues that would be addressed in each section. The description of the section is intended only as a guide when completing the 10 CFR 50.59 documentation and additional information may be warranted. When preparing the 10 CFR 50.59 documentation, it is important to provide sufficient information such that the same conclusion may be reached independently.

## 10 CFR 50.59 Documentation Outline

### *1. Change Description*

A complete description of the change would be provided. Information such as the affected component(s), part(s), and system(s) would be provided. If the change is implemented in redundant channels or trains, that should be noted here as well. Any human-system interface changes should be explicitly described. Also, a brief description of the equipment that is being replaced would be useful. If the change is one in a series of modifications or is part of a global plan for plant modernization, this should be referenced.

### *2. Reason for Change*

This section should discuss the background of the change and why the change is being implemented. Information such as prior system operating and reliability problems, equipment obsolescence, and changing functionality needs would be summarized here. If the change is one in a series of modifications or is part of a global plan for plant modernization, the role of this change in the series of modifications should be discussed. If additional functionality is required by the system as a result of another plant modification, this would also be discussed.

### *3. 10 CFR 50.59 Applicability*

The applicability of 10 CFR 50.59 to the change would be documented here. If there are no changes to the Technical Specifications as part of the change, then this would be noted. Also noted would be confirmation that no other more specific regulations apply to the change.

### *4. Engineering Evaluations*

This section provides detailed justification on why the change is appropriate for the application. The regulatory requirements and industry standards (e.g. General Design Criteria, Regulatory Guides, IEEE standards, etc.) that are met should be identified and credit should be taken for any industry or regulatory guidance that was followed. The justification that any new equipment meets the specified requirements and any other technical evaluations should be provided or referenced. The topics that should be addressed for digital upgrades include, but are not limited to:

- Software life cycle and development process,
- Verification and validation,
- Configuration management,
- Summary of the failure analysis (and specifically, if there are any undetected failures),
- Human-system interface,
- Hardware qualification,
- Internal redundancy and fault tolerance,
- Self-diagnostics,
- Self-tests that perform surveillance testing functions,
- Quality Assurance,
- Electrical or power requirements, and
- Hardware reliability.

### *5. 10 CFR 50.59 Screening Evaluation*

The 10 CFR 50.59 screening evaluation could be provided here. Describing the affected SSC(s) and how the change adversely affects the SSC(s) could help to set the stage for answering the 10 CFR 50.59 evaluation questions. Guidance for screening is provided in Section 4.3 of this guideline.

## 6. Answers to 10 CFR 50.59 Questions

If the change screens out, then this section would not be applicable.

Section 4.4 of this guideline and Section 4.3 of NEI 96-07, Revision 1, provide eight questions that correspond to the eight criteria contained in 10 CFR 50.59(c)(2) for changes that would require a license amendment. If any of the questions were answered yes, then a license amendment would be required to implement the change. Appendix A to this guideline provides a list of issues to consider for each question. A complete discussion that provides the basis for the answer to each question should be provided. In cases where information or discussion applies to more than one question, it is suggested that the applicable information or discussion be documented under each question to provide a complete basis for the answer to each question.

## 7. Conclusions

This section would indicate the result of the screening evaluation and if the change screened in, summarize the answers to the 10 CFR 50.59 questions. If any of the questions were answered "yes," then this section would state that a license amendment pursuant to 10 CFR 50.90 would be required prior to implementation of this modification. If all of the questions were answered "no" (i.e., none of the criteria were met for changes that require a license amendment), and no Technical Specification change is required, then the change may be implemented under 10 CFR 50.59.

## 8. References

Any documentation that would be referenced in the text to support the discussion and the conclusion should be referenced. As a minimum, the section(s) of the UFSAR that apply to the change should be referenced.