



NUCLEAR ENERGY INSTITUTE

proj. 689

**Lynette Hendricks**  
DIRECTOR, LICENSING  
NUCLEAR GENERATION

July 24, 2001

Attention: Document Control Center  
U.S. Nuclear Regulatory Commission  
Washington, DC 20555-0002

**SUBJECT:** Guideline on Licensing Digital Upgrades

The Nuclear Energy Institute (NEI) and EPRI are sponsoring an industry task force to update guidelines for licensing digital system upgrades. The original guidelines for licensing digital system upgrades (EPRI TR-102348) were issued in 1993 and endorsed by the Nuclear Regulatory Commission in Generic Letter 95-02. Since this guideline was originally issued, two fundamental changes have occurred that affect licensing of digital upgrades. First, key guides and standards that provide design requirements for digital-based systems have been reviewed and endorsed by the NRC. Second, 10 CFR 50.59 was revised in 2000 to better define the criteria that establish when prior NRC review is required before implementing plant changes.

Industry plans for updating the licensing digital systems guidelines were discussed with the NRC staff in a public meeting on April 26, 2001. Since that meeting, the task force has completed an initial draft of the updated guideline and that draft is presently being reviewed. We believe that it would be beneficial to afford members of the NRC staff the opportunity to review the current draft of the guidelines. To that end, enclosed please find draft NEI 01-01 (EPRI TR-102348-R1 Draft E July 2001), "Guideline on Licensing Digital Upgrades."

Please provide any comments you may have to the following:

Ray Torok (EPRI) 650-855-2776, [rtorok@epri.com](mailto:rtorok@epri.com)  
Fred Madden (NEI) 202-739-8114, [fwm@nei.org](mailto:fwm@nei.org)

DHk

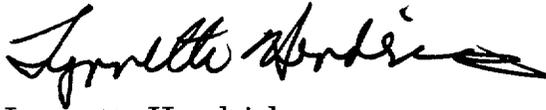


July 24, 2001

Page 2

Please contact me at 202-739-8109 or Fred Madden, if you have any questions.

Sincerely,

A handwritten signature in black ink, appearing to read "Lynnette Hendricks". The signature is fluid and cursive, with a long horizontal stroke at the end.

Lynnette Hendricks

FWM/

Enclosure

c: Mr. J. A. Calvo, USNRC MS: OWFN 9D4  
Mr. E. C. Marinos, USNRC MS: OWFN 11D19  
Ms. E. M. McKenna, USNRC MS:OWFN 11E8  
Mr. P. C. Wen, USNRC MS:OWFN 11F1



# **Guideline on Licensing Digital Upgrades**

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

**NEI 01-01**

**EPRI TR-102348-R1 Draft E, July 2001**

**This project was co-sponsored by the U.S. Department of Energy and the Electric Power Research Institute**

**Prepared by  
A Joint Task Force of  
The Nuclear Energy Institute  
and  
The Electric Power Research Institute**

## **DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES**

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

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

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

ORGANIZATION(S) THAT PREPARED THIS DOCUMENT

**MPR Associates, Inc.**

## **ORDERING INFORMATION**

Requests for copies of this draft report should be directed to the EPRI Project Manager, R. Torok, P.O. Box 10412, Palo Alto, CA 94303-0813, (650) 855-2776, [rtorok@epri.com](mailto:rtorok@epri.com).

Electric Power Research Institute and EPRI are registered service marks of the Electric Power Research Institute, Inc. EPRI. POWERING PROGRESS is a service mark of the Electric Power Research Institute, Inc.

Copyright © 2001 Electric Power Research Institute, Inc. All rights reserved.

# ACKNOWLEDGEMENTS

---

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.
Kristin Davis	MPR Associates, Inc.
Ray DiSandro	Exelon Nuclear
Larry Erin	Westinghouse
Bob Fink	MPR Associates, Inc.
Wayne Glidden	First Energy 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.
Fred Madden	Nuclear Energy Institute
Jerry Mauck	Framatome ANP
Wade Messer	Duke Energy
Joseph Naser	Electric Power Research Institute
Denny Popp	Westinghouse
Roy Raychaudhuri	Sargent and Lundy
Joe Ruether	Excel Energy
Clayton Scott	Invensys/Triconex
Rob Slough	TXU Electric
Jack Stringfellow	Southern Nuclear
Dinesh Taneja	Bechtel Power Corp.
Ray Torok	Electric Power Research Institute

# CITATIONS

---

[LATER]

# REPORT SUMMARY

---

[LATER]



---

# ABSTRACT

---

[LATER]



---

# CONTENTS

---

<b>1 INTRODUCTION .....</b>	<b>1-1</b>
1.1 Background.....	1-1
1.2 Purpose of This Guideline .....	1-2
1.3 Contents of This Guideline .....	1-3
<b>2 DEFINITIONS AND TERMINOLOGY .....</b>	<b>2-1</b>
<b>3 DIGITAL UPGRADE PROCESS .....</b>	<b>3-1</b>
3.1 Digital Upgrade Process Overview.....	3-1
3.1.1 Digital Issues in the Upgrade Process .....	3-3
3.1.2 Failure Analysis .....	3-3
3.2 Phases of the Upgrade Process.....	3-5
3.2.1 Project Definition and Planning.....	3-5
3.2.2 Requirements .....	3-6
3.2.3 Design and Implementation .....	3-7
3.2.4 Testing, Installation, and Commissioning.....	3-7
3.2.5 Operation, Maintenance, and Support.....	3-7
<b>4 LICENSING PROCESS AND 10 CFR 50.59 .....</b>	<b>4-1</b>
4.1 Review for Potential Tech Spec Changes .....	4-3
4.2 50.59 Screening.....	4-3
4.2.1 Technical Evaluations.....	4-6
4.2.2 Screening Human-System Interface Changes.....	4-10
4.3 10 CFR 50.59 Evaluation .....	4-11
4.3.1 Does the activity result in more than a minimal increase in the frequency of occurrence of an accident?.....	4-11
4.3.2 Does the activity result in more than a minimal increase in the likelihood of occurrence of a malfunction of an SSC important to safety? .....	4-12
4.3.3 Does the activity result in more than a minimal increase in the consequences of an accident? .....	4-14

4.3.4 Does the activity result in more than a minimal increase in the consequences of a malfunction? .....	4-14
4.3.5 Does the activity create a possibility for an accident of a different type? .....	4-14
4.3.6 Does the activity create a possibility for a malfunction of an SSC important to safety with a different result? .....	4-15
4.3.7 Does the activity result in a design basis limit for a fission product barrier being exceeded or altered? .....	4-18
4.3.8 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? .....	4-18
4.4 License Amendment Process .....	4-18
4.4.1 No Significant Hazards Consideration .....	4-19
4.4.2 Environmental Considerations .....	4-20
<b>5 FAILURE ANALYSIS .....</b>	<b>5-1</b>
5.1 Identification of Potential System-Level Failures and their Consequences .....	5-2
5.2 Identification of Potential Causes of System Failures .....	5-4
5.3 Assessment of the Significance and Risk of Identified Failures .....	5-6
5.4 Identification of Appropriate Resolutions for Identified Failures .....	5-9
<b>6 ADDITIONAL GUIDANCE ON ADDRESSING DIGITAL UPGRADE ISSUES .....</b>	<b>6-1</b>
6.1 Background on Digital Quality and Dependability Issues .....	6-1
6.2 Safety Significance and Complexity .....	6-2
6.3 Digital System Quality .....	6-3
6.3.1 Software Life Cycle and Development Process .....	6-5
6.3.2 Types of Software in Digital Systems .....	6-5
6.3.3 Software Verification and Validation .....	6-6
6.3.4 Software Configuration and Change Management .....	6-7
6.3.5 Software Safety Analysis .....	6-7
6.3.6 Use of Commercial Off the Shelf (COTS) Equipment .....	6-7
6.4 Digital System Design and Performance .....	6-8
6.4.1 Hardware Qualification .....	6-8
6.4.2 Human Factors .....	6-9
6.4.3 System Integrity and Failure Management .....	6-10
6.4.4 Real-Time Performance .....	6-10
6.5 Defense-in-Depth and Diversity .....	6-11
6.5.1 Applicability of Defense-in-Depth and Diversity Requirements .....	6-12
6.5.2 Defense-in-Depth and Diversity Analysis Methods .....	6-13

---

6.5.3 Diversity Required by the ATWS Rule .....	6-13
6.6 Dependability and Software Common Mode Failure.....	6-14
6.6.1 Evaluation of Software Dependability .....	<b>Error! Bookmark not defined.</b>
<b>7 REFERENCES .....</b>	<b>7-1</b>



---

# LIST OF FIGURES

---

Figure 3-1. Digital Upgrade Process .....	3-2
Figure 3-2. Using Failure Analysis to Understand and Control Risk .....	3-5
Figure 4-1. 10 CFR 50.59 Process (from NEI 96-07, Revision 1) .....	4-2
Figure 4-2. 10CFR50.59 Screening .....	4-5
Figure 4-3. Technical Evaluation and 10 CFR 50.59 .....	4-6
Figure 4-4. Applicability of Defense-in-Depth and Diversity Requirements .....	4-7
Figure 4-5. Developing Reasonable Assurance That Risk of Failure is Low .....	4-8
Figure 5-1. Functions and Failures at Different Levels .....	5-2
Figure 6-1. Applicability of Defense-in-Depth and Diversity Requirements .....	6-12



# 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 special Nuclear Regulatory Commission (NRC) scrutiny.

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 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 clearly 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

---

## *Introduction*

complement NEI 96-07 with guidance for digital upgrade issues. Other changes were made to address key digital issues in the context of the technical 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.”
- 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 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 properly assess the potential for and impact of failures, a failure analysis with an appropriate level of detail is needed.
- This guideline should provide a road map to relevant standards and other guidelines that can be applied in addressing digital upgrade issues, providing references to industry standards, guidelines, EPRI reports, regulatory requirements, and other documents as appropriate for addressing the issues.

## **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 for digital upgrades 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.

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. Also, the guidance is not limited to instrumentation and control systems; it could apply 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” upgrades; that is, changes that may be required after analog equipment is replaced with a digital-based system.

### **1.3 Contents of This Guideline**

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. Guidance on failure analysis is discussed in the context of the design and design verification processes.

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.

Guidance on performing failure analyses is provided in Section 5. A variety of examples are included to illustrate failure analysis concepts and how the results are used in design and licensing.

Section 6 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 evaluations needed to support the 50.59 process.

# 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). [NEI 96-07, Revision 1]

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

---

## Definitions and Terminology

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 must be 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 protection, trip, or scram system; the Engineered Safety Features Actuation System (ESFAS); the Anticipated Transients Without Scram (ATWS); and the monitoring and indicator system. 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]

**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) or in the *equipment* (hardware and/or software) used to perform the function. [Derived from IEC 880 and the EPRI Equipment Qualification Reference Manual TR-100516]

**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]

**Failure.** See Malfunction.

---

*Definitions and Terminology*

**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.). Currently the term synonymous with and replacing human-machine interface (HMI) and man-machine interface (MMI).

**Malfunction.** In the context of 50.59, malfunction means the failure of a structure, system, or component to perform its intended design functions 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]

**Safety related.** See safety systems.

**Safety systems, structures, and components.** 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 10 CFR Part 100 guidelines. [IEEE 603-1991]

**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.

**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 upgrade 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 any changes to the plant processes that may be needed to support the digital upgrade process.

First, a general overview is given which describes the modification process, failure analysis and its role in design and licensing, and the treatment of digital upgrade issues. Then, guidance is provided for some of the important steps in the 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. Also, activities associated with design reviews and verification and validation (V&V) are not shown on the diagram (see Annex E of IEEE 7-4.3.2-1993 for more details).

The upper right portion of the diagram shows activities associated with evaluation of potential system failures. In order to assess the impact of any change 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.

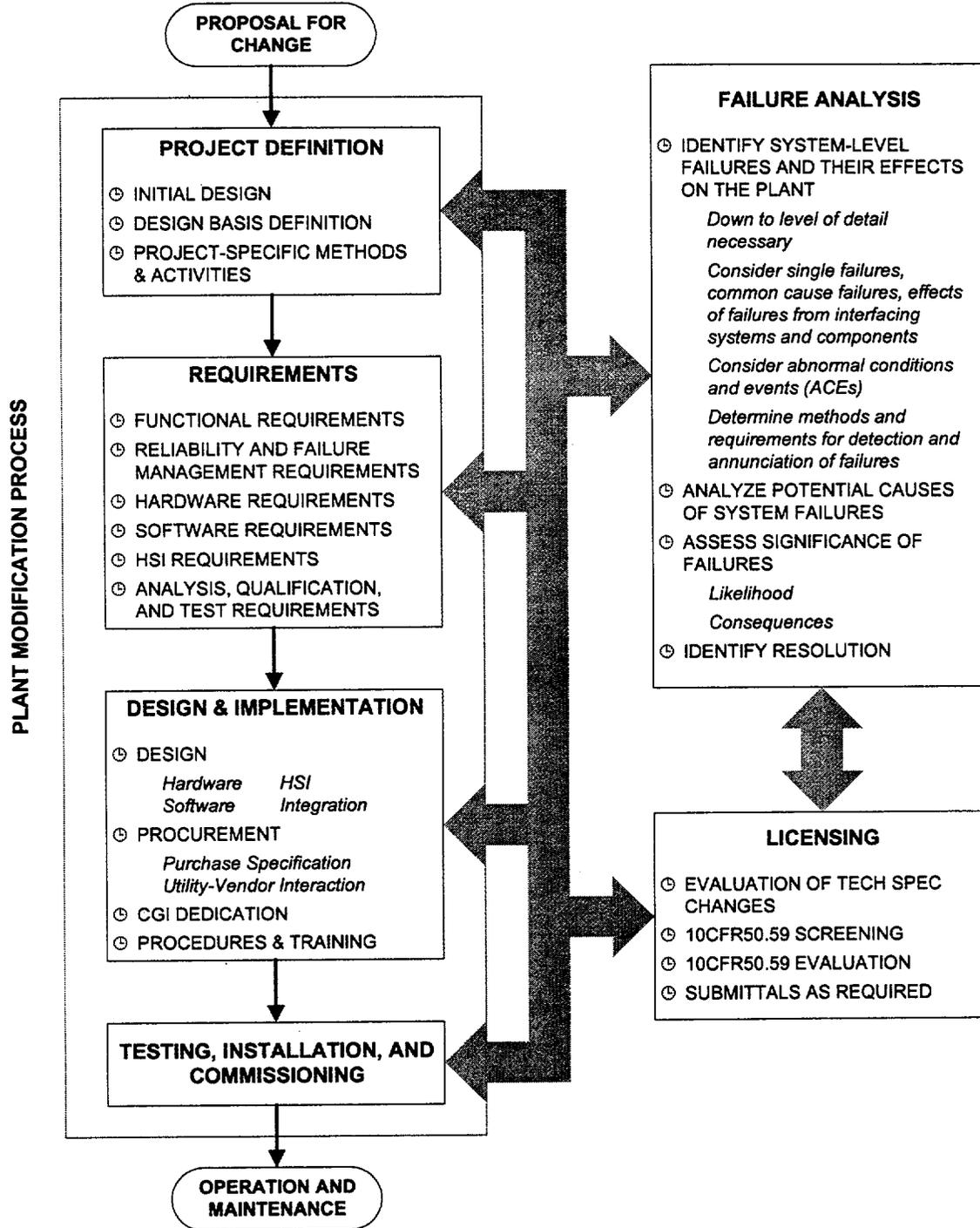


Figure 3-1. Digital Upgrade Process

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 and licensing activities. This is important because many of the questions addressed in licensing (e.g., 10 CFR 50.59 questions regarding potential new failure modes) can be resolved using information that comes out of the failure analysis. This is discussed further in Section 5.

### **3.1.1 Digital Issues in the Upgrade Process**

Some of the key design issues for digital systems, including software quality, defense in depth, and the human-system interface (HSI), are addressed at a number of points in the process of specifying, designing, and implementing a digital upgrade. For example, requirements on the development and quality assurance of software should be specified, software safety analysis performed, and software verification and validation activities carried out throughout the design, implementation, testing, installation, commissioning, and long-term maintenance of the upgrade. Similarly, HSI design requirements need to be specified, appropriate validations and verifications performed, and necessary training, procedures, and administrative controls provided to ensure adequate protection 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. Note that the failure analysis is separate and distinct from the defense-in-depth and diversity analyses that may be expected for certain large scale safety system upgrades (see Sections 4.2 and 6.5).

### **3.1.2 Failure Analysis**

Initially, failure analysis provides input in the form of design requirements (e.g., 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 of this guideline provides more detailed guidance for performing failure analyses.

Resolution of potential failure modes and hazards typically involves engineering judgment, with consideration of several contributing factors. These 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 annunciating the failure to the operator, maintenance and plant operation requirements to repair the failure. If the potential failure mode or hazard is judged to be significant, the resolution may be to add system design features that preclude or protect against the failure, to take credit for backup from another system (defense in depth), to take actions that reduce the likelihood of the failure, or, if the problem is a lack of data to support an assessment of the likelihood of failure,

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 mitigate 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 either in the region of negligible or acceptable risk.

At the engineering design stage, consequences could involve both safety and economic aspects. For regulatory purposes only the safety consequences are important. For this diagram, 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, fault tolerance, operating history, device complexity, system complexity, and testability. Plant PRA data could also contribute to the assessment. These elements of dependability are discussed further in Section 6.

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 mode failure) and it applies regardless of whether the change under consideration affects an entire system or is only a component-level change.

While it is performed as part of the design process, failure analysis also provides important input to the 10 CFR 50.59 process, particularly regarding the effects of the digital upgrade and its potential failures on the function of the system. Here it is important to maintain focus at the level of the of the design functions performed by the system, because it is the effects of failures on the system and the resulting impact on the plant that are important.

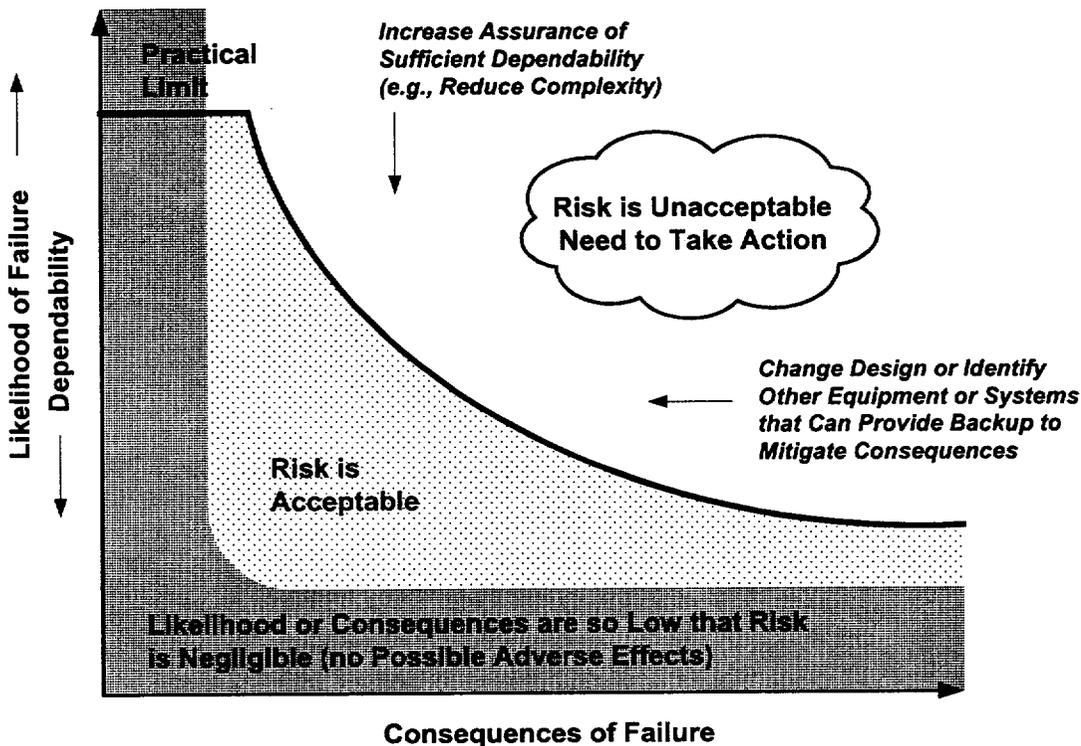


Figure 3-2. Using Failure Analysis to Understand and Control Risk

## 3.2 Phases of the Upgrade Process

The phases of the upgrade process shown in Figure 3-1 are discussed below, along with specific guidance related to digital upgrades. EPRI 1001045 provides more detailed guidance on important issues to consider in each of these phases.

### 3.2.1 Project Definition and Planning

The types of activities to be performed and the methods and techniques to be applied in the design and implementation 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 (particularly the existing plant procedures and practices that can be applied and types and methods for new procedures),
- failure analysis methodology and specific analysis techniques,

---

### *Digital Upgrade Process*

- software development methodology,
- tools and techniques for verification and validation, and
- levels of independence for verification, validation, and safety analysis.

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.

### **3.2.2 Requirements**

Experience in previous digital upgrades and lessons learned from software development and use in general have shown that proper specification of software requirements is a key element in assuring adequate performance of the system. 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.

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.

### **3.2.3 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 specific digital platform is evaluated and selected based on the requirements, hardware qualification tests are performed as necessary, commercial grade item dedication is performed, and application software is developed, recognizing that some of these choices may 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 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 6.

### **3.2.4 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. These activities are critical in verifying the adequacy of the design and treatment of the digital upgrade issues. 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 also helps with human-system interface verification and validation. 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.

### **3.2.5 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 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. This includes identifying changes required to existing procedures and any new procedures that will be required to support configuration, operation, maintenance,

---

### *Digital Upgrade Process*

and modification of the upgraded equipment, including software safety analysis, software and hardware maintenance, and 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 (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.

# 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 some specific considerations that should be addressed when making digital upgrades regarding the 10 CFR 50.59 criteria. These considerations include 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 shown in Figures 4-1 and 4-3, technical evaluations are necessary inputs to the 50.59 process. For digital upgrades, these evaluations include assessments of dependability (see Section 6.6) and failure analyses (Section 5). Failure analysis identifies potential failures, assesses their consequences and significance, and determines appropriate resolutions, commensurate with the safety significance of the modified system as described in the UFSAR.

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 3.2.1) before extensive dialogue is initiated.

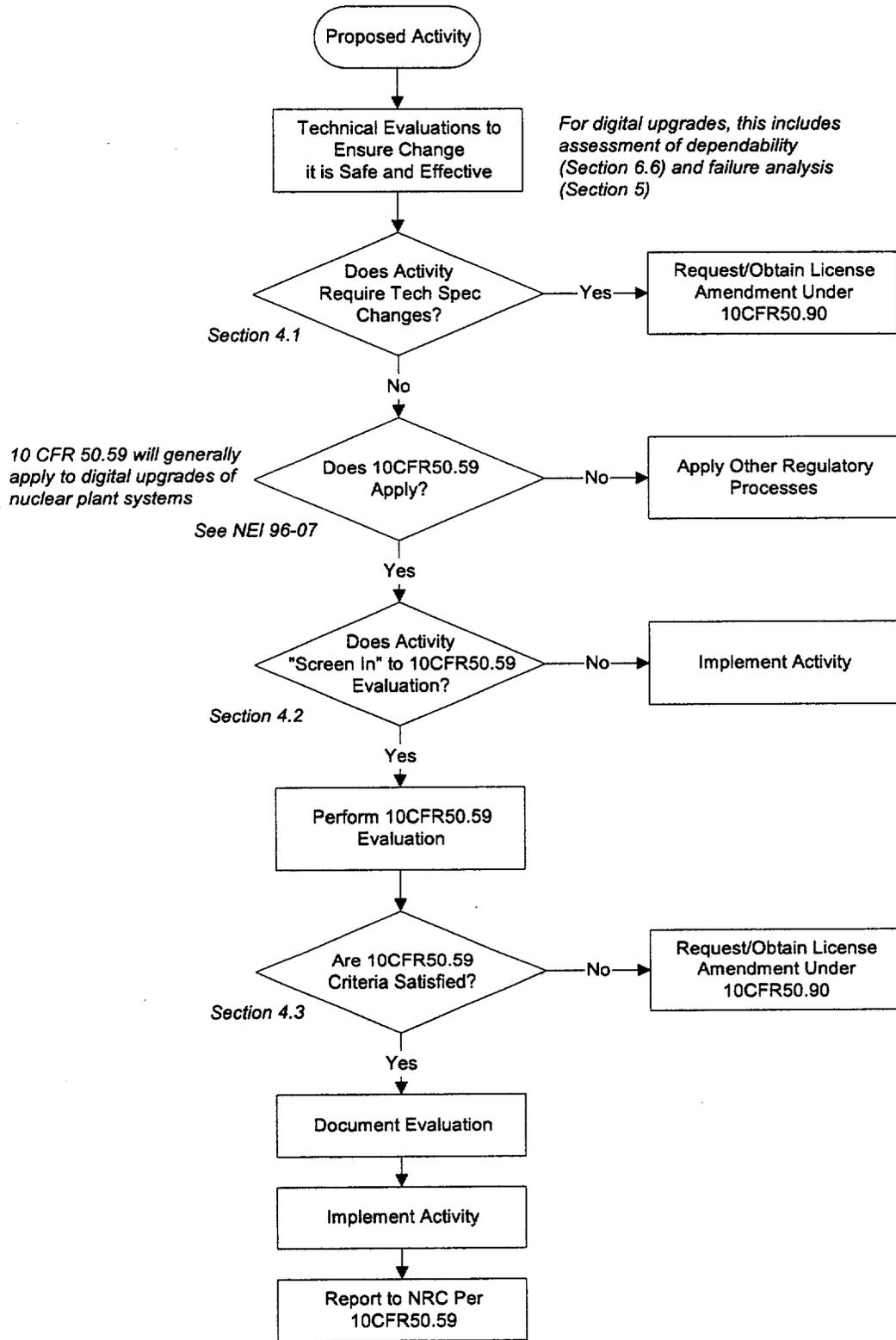


Figure 4-1. 10 CFR 50.59 Process (from NEI 96-07, Revision 1)

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

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. 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.

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.

#### **4.2 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 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.

Figure 4-2 provides an overview of the thought process involved in 10 CFR 50.59 screening. In the context of 50.59 screening, the first step 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 50.59 process. If the changes 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 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, and
- Adversely affecting the response time required to perform required actions.

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

The following section describes how the Technical Evaluation interfaces with the 10 CFR 50.59 screening and evaluation process.

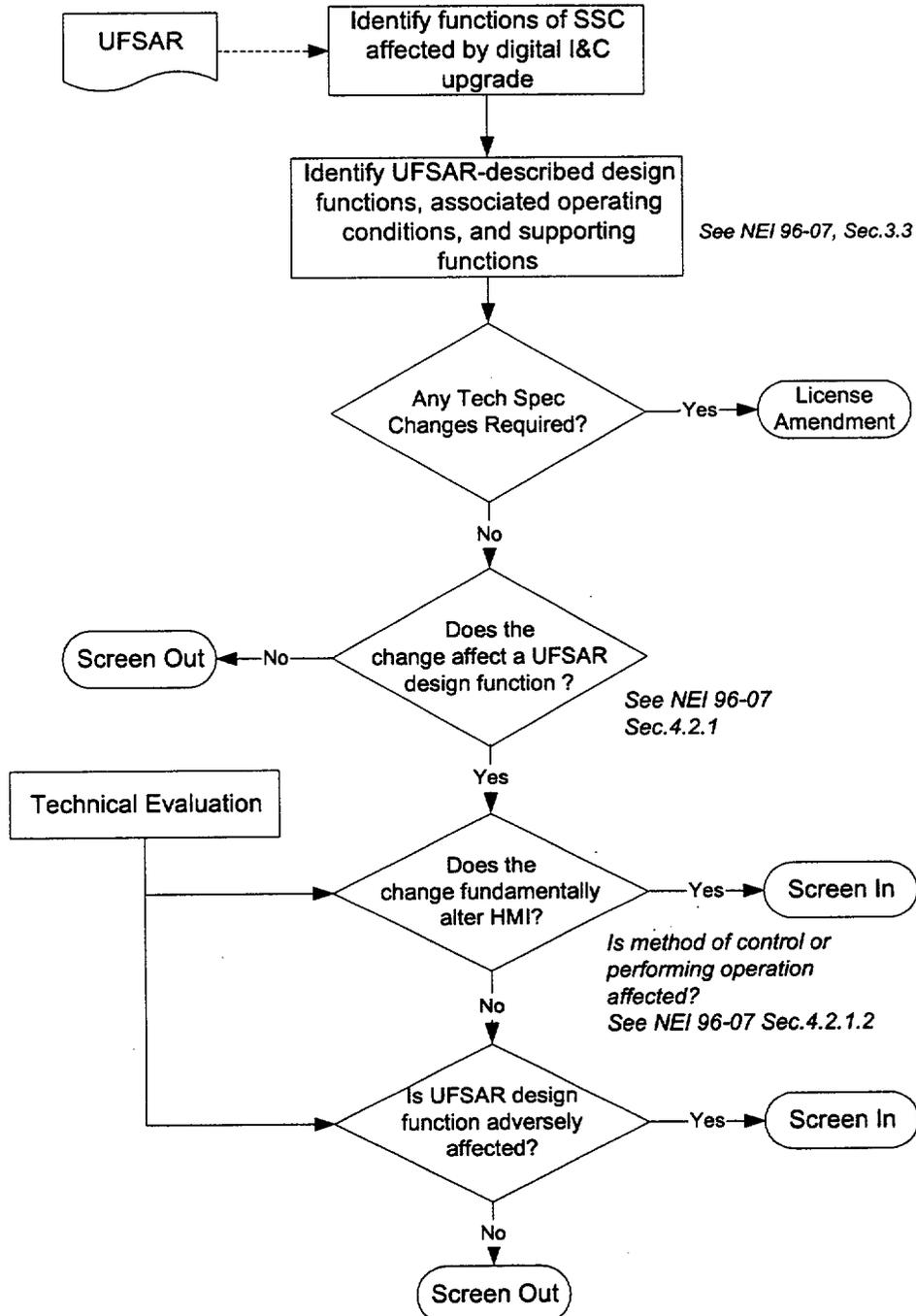


Figure 4-2. 10CFR50.59 Screening

### 4.2.1 Technical Evaluations

Addressing most design issues, such as the bullet items listed above, is relatively straightforward for hardware-only changes. However, for digital upgrades the challenge is addressing the effect of software on reliability of the design function. The answer lies in the technical evaluations that are performed throughout the modification process. As illustrated in Figure 4-3, these technical evaluations include such activities as evaluating the dependability of the digital equipment and its associated software per Section 6.6, and by analyzing potential failures per Section 5.

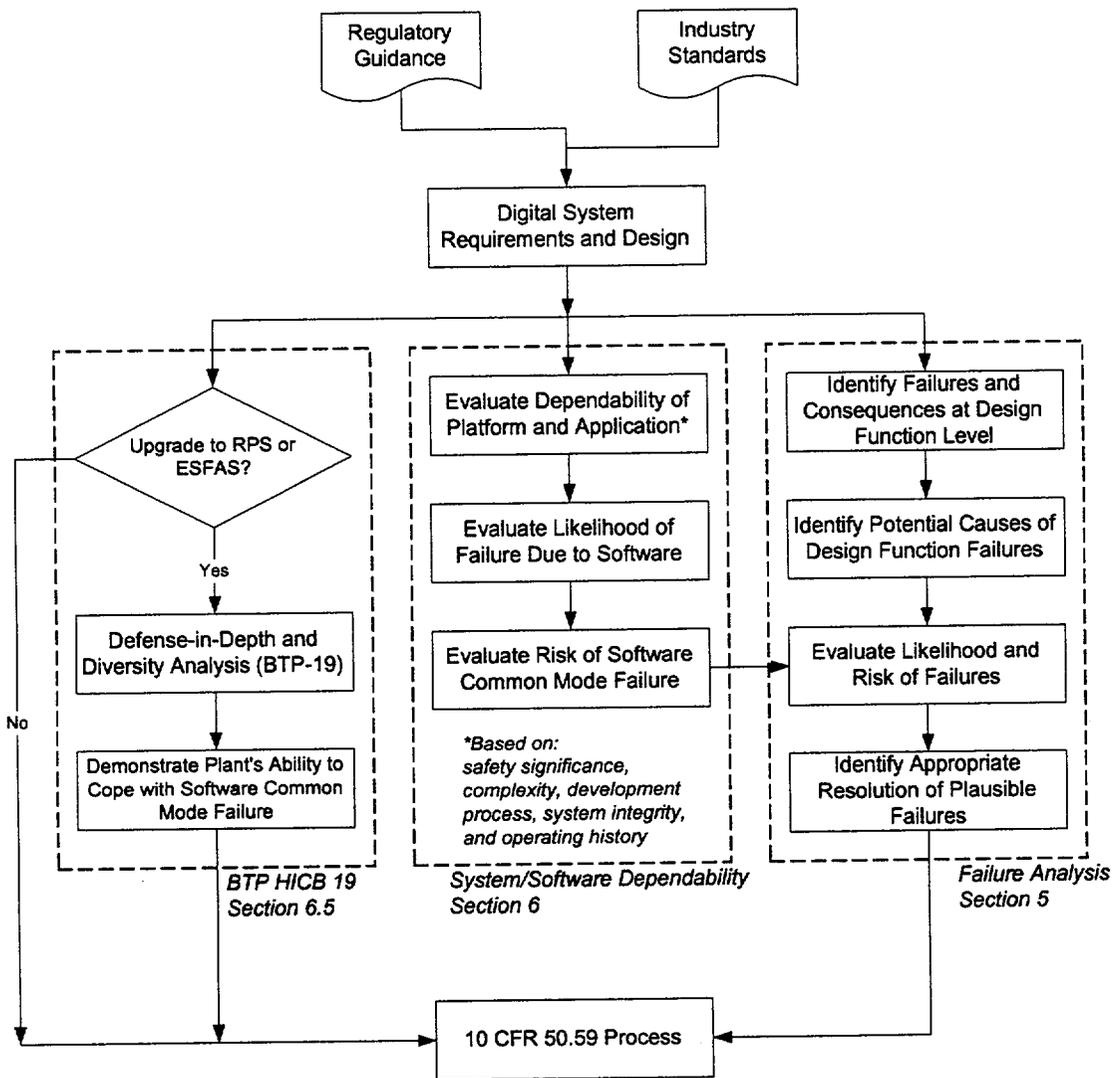


Figure 4-3. Technical Evaluation and 10 CFR 50.59

In addition, a defense-in-depth and diversity analysis is expected for substantial reactor protection system (RPS) and emergency safety features actuation system (ESFAS) upgrades, as illustrated in Figure 4-4 and discussed in Section 6.5. This analysis is used to demonstrate the plant's ability to cope with a postulated common mode failure that disables all redundant processing channels.

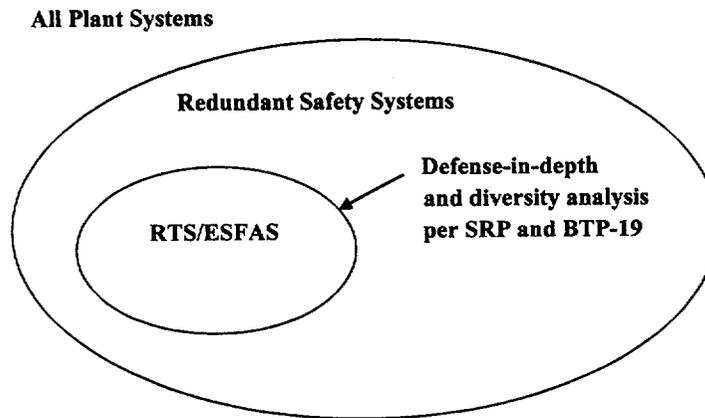


Figure 4-4. Applicability of Defense-in-Depth and Diversity Requirements

Results of these technical evaluations can then be 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 so low that the risk is negligible, and compliance is shown with all applicable codes, standards, and regulatory documents, then no adverse effects are created and the change should screen out.

For some relatively simple digital equipment, the technical evaluation 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 Sections 5 and 6, consensus methods have been developed for evaluating dependability of digital equipment including assessment of the potential common mode failure due to software. Some vendors are using updated and improved processes for software and digital system development, V&V and configuration management. And some digital equipment has gained extensive operating history, both inside and outside the nuclear industry.

Simplicity of the device and application (in terms of inputs/outputs, digital processing and software architecture, etc.), combined with a good development process meeting industry standards and regulatory guidance, plus extensive and relevant operating history, should result in reasonable assurance that failure due to software is no more likely than other potential failures such as common mode hardware failures, calibration/maintenance errors, etc., that have not been considered in the UFSAR. In such cases, no further consideration of software-based failures, including software common mode failures, would be warranted and no defense-in-depth and diversity analysis would be required (see Example 4-3). (In fact, 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.) The change would screen out of 50.59.

In addition to the software question, other characteristics of a digital upgrade could cause the change to screen in to a 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 below 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.

Figure 4-5 provides a simplified illustration of how reasonable assurance that the risk of failure is low may be obtained through a combination of activities, such as evaluating operating history and quality, failure analysis, and defense-in-depth and diversity analysis. The following examples illustrate typical screening considerations for a small digital upgrade.

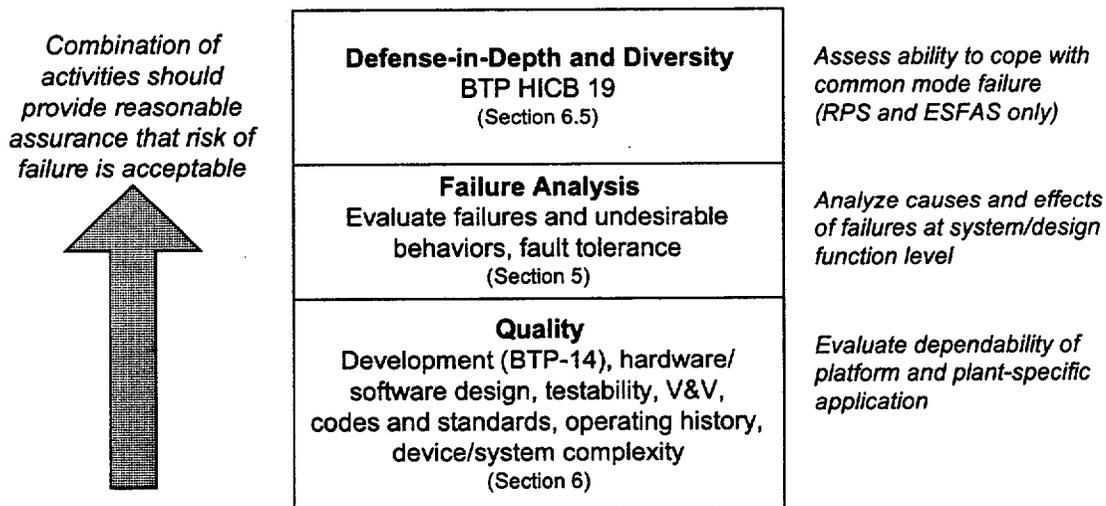


Figure 4-5. Developing Reasonable Assurance That Risk of Failure is Low

**Example 4-1. 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 will also meet all current required performance, HSI, and qualification requirements, and will have no new failure modes or effects at the level of the design function. The licensee thus concluded that the change would not adversely affect any design function and screened out the change.

---

---

**Example 4-2. Screening for a Recorder Upgrade (Screens In)**

Similar to Example 4-1, a licensee is replacing an analog recorder with a new microprocessor based recorder. However, in this instance, the engineering/technical evaluation determined that the 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 concluded that there would be an adverse effect on an UFSAR-described design function and screened in the change. In the 50.59 evaluation, the licensee evaluates the magnitude of this adverse effect.

---

---

**Example 4-3. 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 being 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.

A technical evaluation of the new device concludes that it was 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 is 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 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 since the change involves component replacement and not a change to the system architecture, the change is not considered to be substantial, and falls outside of the inner circle of Figure 4-4. Therefore, a defense-in-depth and diversity analysis is not necessary.

---

### **4.2.2 Screening Human-System Interface Changes**

In the discussion of the screening process regarding performing or controlling design functions, NEI 96-07, Rev. 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.”

However, minor changes in the human-system hardware interface that may accompany a digital upgrade do not necessarily screen in, requiring a 50.59 evaluation. Instead, 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). Section 6.4.2 provides guidance on human factors considerations for the design and the failure analysis. Characteristics of HSI changes that could lead to potential adverse effects may include, but are not limited to:

- Changes in the basic sequence of control of plant equipment and systems during transients (including parameters monitored, decisions made, and actions taken),
- 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 any of 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 errors.

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 50.59 evaluation is required.

However, 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.

### **4.3 10 CFR 50.59 Evaluation**

NEI 96-07, Revision 1, provides general guidance for preparation of 10 CFR 50.59 evaluations. Section 4.3 of NEI-96-07 presents the eight 10 CFR 50.59 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.

#### **4.3.1 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 that are 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, as considered by the following:

- 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 can use PRA calculations to assess the change in probable frequency of events. 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 change would not be expected to result in more than a minimal increase in the likelihood of occurrence of an accident.

#### **4.3.2 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 evaluate potential failures of structures, systems, and components (SSCs) to perform their design function as described in the UFSAR, and whether the causes of such failures are affected by the proposed change. 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.

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

It is important to note that digital equipment failure is credible, but the likelihood of such failures causing malfunctions of the system in which it is installed may be "minimal" to the extent that it does not change 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) is needed to understand how the 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. If digital device failures can cause the system to

malfunction, an evaluation of dependability (discussed in Section 6.6) is needed to assess whether the likelihood of malfunctions has increased.

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. A digital device developed in accordance with a defined life cycle process, with good failure management features and successful operating history, and complying with the applicable industry standards and regulatory guidance discussed in Section 6 should not increase the likelihood of malfunctions.

Appropriately implemented self-diagnostic features can also reduce the likelihood of system malfunctions by alarming failures of the digital equipment to the operators. As a result, timely corrective action can be taken before the plant system is called upon to perform its design function or before additional failures place the plant in an unanalyzed state.

Per NEI 96-07, if the uncertainty in assessing the likelihood of system malfunction is such that it cannot reasonably be determined that the likelihood increases (i.e., no clear trend), then the change is considered minimal. Also per NEI 96-07, changes that reduce redundancy, diversity, separation, or independence are considered to result in more than a minimal increase in the likelihood of occurrence of malfunctions. The failure analysis, and for RPS and ESFAS the BTP-19 defense-in-depth and diversity analysis, should provide the insights needed to determine if the change reduces redundancy, diversity, separation, or independence.

---

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

A PLC is to be installed to replace analog equipment that monitors some equipment in the chemical and volume control system. The PLC has been "pre-qualified" and the NRC has issued an SER concluding that the PLC is suitable for use in safety-related applications. The application is simple (monitoring several analog inputs and generating alarm outputs based on water level and temperature). Because of its simplicity, there is high confidence that the application can be thoroughly tested. However, because this is the first instance in which this PLC is applied to this particular application, the change is conservatively screened in to the 50.59 process.

The 50.59 evaluation concluded that the dependability of the system (based on pre-qualification of the platform plus simplicity and testability of the application) provides reasonable assurance that malfunctions, including failure due to software, will be highly unlikely, and no more likely than with the present analog system. Also, no new malfunctions with a different result are created. Therefore, the change can be implemented under 50.59. Note that the next time the pre-qualified PLC is used in the same application, it may screen out if the operating history is positive.

---

---

**Example 4-5. Likelihood of Malfunctions for a Single Train System**

The controls for the Turbine Driven Auxiliary Feedwater Pump (TDAFP) are being converted from analog to digital. This single pump provides backup to the two motor driven Auxiliary Feedwater Pumps that use different controls, and therefore there is no concern with common mode failure issues. The TDAFP controls are highly dependable, and the same digital equipment has been used for turbine control in many other similar applications. The 50.59 evaluation concludes that the dependability of the system (based on quality development process, fault tolerant design, and good operating history) is sufficient to demonstrate low likelihood of malfunctions. Therefore, the change can be implemented under 50.59.

---

**4.3.3 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.

**4.3.4 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.

**4.3.5 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?

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

This addresses results or effects of potential system failures, and whether the effect is bounded by failures explicitly described in the UFSAR. The evaluation needs to compare results of malfunctions evaluated in the UFSAR with the results of failure modes that the proposed activity could create. The key issue here is the effect of failures of the digital device on the system in which it is installed. The failure analysis (Section 5) 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, this upgrade would not create malfunctions with a different result.

As discussed above for Criterion 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.

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 50.59 evaluation, “credible” malfunctions are defined as those as likely as the malfunctions assumed in the UFSAR.

Results of the failure analysis should be used to identify the effects of “credible” failures on the design function of the system. The effects of these failures should be compared to the failures addressed or assumed as part of the safety analyses in the UFSAR. On the basis of the evaluation of likelihood of malfunction (Criterion 2), if there is reasonable assurance (see Figure 4-5) 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 “credible,” 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 back ups to mitigate potential adverse impacts on design functions, then for the purposes of the 50.59 evaluation, there would be no new outcome, and the change would be implemented under 50.59. The 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.

When a defense-in-depth and diversity analysis is performed (see Figure 4-4 and the discussion in Section 6.5), the results should be discussed to address the effects of common-mode failure. Satisfactory compliance with BTP-19 indicates that the potential consequences of common mode failure have been reduced to a level that presents acceptable risk. Consequently, if the BTP-19 criteria are met and the analysis employed a generic, pre-approved defense-in-depth and diversity approach, tailored to address plant-specific conditions, then the change would be implemented under 50.59. The 50.59 evaluation would describe the back up for addressing software common mode failure, along with the licensing commitments it entails. If the BTP-19 criteria are not met (e.g., RPS and ATWS are not diverse), or a method other than that described in BTP-19 is used to address software common mode failure, then a license amendment would be required.

In addition to software common mode failure, 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.

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 50.59 evaluation (e.g., the likelihood and results of malfunctions due to these additional changes should also be addressed).

---

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

The PLC used in Example 6-1 for a EDG load sequencer application is to be used to replace the analog logic and relay actuation portions of the ESFAS system. This application is relatively complex in terms of the number of functions, inputs, and outputs. The application also takes advantage of the digital system's expanded capabilities by including new logic to implement system diagnostics and periodic surveillance testing functions. This upgrade is also the first ESFAS application using this PLC.

The change screens in, and the 50.59 evaluation concludes that because of the complexity (e.g., new automated testing features) and lack of operating experience with the application, the threat of common mode software failure is credible. The defense-in-depth and diversity analysis per BTP-19 demonstrates that there is sufficient backup capability to cope with software common mode failure, thus the risk posed by such failure is acceptable. However, the analysis relies on best-estimate analysis techniques that have not been previously approved by the NRC. Accordingly, prior NRC review of the proposed change will be required. NRC approval of the analysis method is obtained with this first application, therefore subsequent upgrades using the same approach might be implemented without prior review.

---

#### **Example 4-7. Malfunctions with no Different Results**

A digital single loop controller is being installed in redundant HVAC control loops for the electrical equipment room. The commercial dedication of the controller identifies some shortcomings in the development process (lack of design documentation and V&V records). Therefore, the change is screened in. In the 50.59 evaluation, common mode failure due to software is considered "credible" and the consequences of such failure are evaluated. The evaluation concludes that in the event of failure, a halt in processing would be alarmed and diverse equipment would alarm any significant increase in ambient temperature. The operators could then de-energize and re-boot the controllers from the main control room. The time to alarm, recognize the problem, and re-boot the controllers is a maximum of ten minutes based on simulator testing and bench testing of the controller. The time for the room to heat up from its normal temperature setpoint to its allowable temperature of 120°F is 20 minutes. No substantial changes are needed to equipment or procedures to provide the needed back up capability. The operator has sufficient time to reset the controls within the bounds of the current licensing basis and without impacting equipment served by the HVAC unit. It is concluded that there are no malfunctions with different results, and the change is performed under 50.59.

---

#### **4.3.7 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 directly 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. The design basis limits may be affected if the timing (response or processing) of the digital device is different than 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.

#### **4.3.8 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 the safety analysis is acceptable. NEI 96-07, Revision 1 indicates that changes 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 NRC, constitute a departure from a method of evaluation described in the UFSAR.

### **4.4 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 4.4.1);
- Environmental Considerations, documentation of categorical exclusion pursuant to 10 CFR 51.22 (see Section 4.4.2)

Additional documentation that should be available, 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 verification and validation activities and configuration management process for the new design;
- Test Program Summary, including discussion of factory acceptance, integration, installation, surveillance, and time response tests;
- Compliance with hardware qualification requirements;
- Description of the hardware, firmware, and software;
- 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.

#### **4.4.1 No Significant Hazards Consideration**

Section 4.0 of the NEI white paper addresses the significant hazards consideration, pursuant to 10CFR50.92, "Issuance of Amendment", through three questions corresponding to the three criteria in 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 50.59(c)(2)(i) and (iii), corresponding to the questions in Sections 4.3.1 and 4.3.3 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 reliability should be evaluated. System software verification and validation (V & V) and equipment hardware qualification (seismic, environmental, EMI) play a part in reliability.

The consequences of an accident refer to the release of radiation dose to the public. Systems that provide accident mitigation functions will 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 50.59(c)(2)(v), corresponding to the question in Section 4.3.5 regarding a new or different kind of accident. Question 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, set points, response times, or design parameters. NRC notes in the Federal Register notice regarding the final 50.59 rule (Reference 25) 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 (50.59(c)(2)(vii) criteria, or the question in section 4.3.7) or
- a departure from a method of evaluation described in the UFSAR used in establishing the design basis or safety analysis (50.59(c)(2)(viii) criteria or the question in section 4.3.8).

#### **4.4.2 Environmental Considerations**

10CFR51.22, "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 10CFR51.22(c)(9). Therefore, the statement suggested by the NEI white paper corresponding to 10CFR51.22(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 10CFR50.92 (see guidance in Section 4.4.1 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 system affected by the upgrade on the type or amount of effluent should be considered. Changes to parameters such as set points, measurement accuracy, changes in sampling equipment, and response times 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 10CFR51.22.

# 5

## FAILURE ANALYSIS

---

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 not 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 6.3.5, 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:

1. 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.
2. Identification of potential vulnerabilities, which could lead to system failures or undesirable conditions.
3. Assessment of the significance and risk of identified vulnerabilities.
4. 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 Identification of Potential System-Level Failures and their Consequences

Ultimately, the digital equipment is installed to support overall I&C 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.

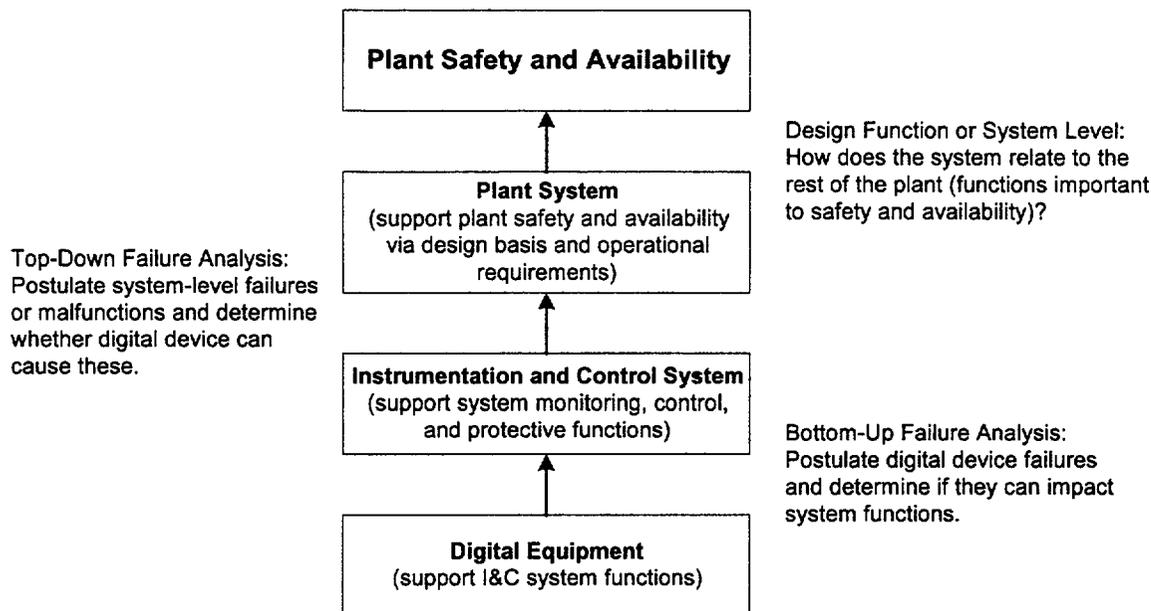


Figure 5-1. Functions and Failures at Different Levels

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 (see Section 4).

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 can 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. It is determined 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 is 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.)

---

## **5.2 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 Section 6.6 for guidance on when software should be considered a plausible cause of a common mode 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.

---

### **5.3 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 6) or using conservative bounding levels for failure probability as appropriate. Dependability evaluations are discussed in detail in Section 6.6.

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.

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 5-3. 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 are 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 probability of a software common cause failure causing a failure to trip on demand cannot be established with present methods, based on the evaluation of the software and its operating experience described above, it is concluded that the probability of such a failure is much less than  $P$  (say an order of magnitude less). The probability of a failure to trip is 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.

---

### **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 are to be replaced during an outage. Mechanical governors, which normally function as actuators for the electronic governors, also are 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 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. 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, it is concluded 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, it is concluded that software common cause failures in the new governors are 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 is carried out under 10 CFR 50.59.

---

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

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

1. 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.
2. 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 would 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.
3. Rely on existing systems and defense in depth 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 it may include use of non-safety-related equipment. Note that, if the failure has not been analyzed previously, this may represent a malfunction with a result different than those analyzed in the UFSAR.
4. Supplement the defense in depth offered by existing systems, procedures, and/or training 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, to provide a means of prompt repair of the fault.

Example 5-5 discusses the failure analysis for replacement of a simple, proven instrumentation device 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 are 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 change is carried out 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 are 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, because of the complexity of the design including the software, the particular system architecture used and the difficulty in managing failures within the system, the potential for a common cause failure due to software could be a concern in that it could lead to loss of one of the primary protection functions provided by the ESFAS. It is determined 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, requiring a license amendment.

At this point the licensee considers a number of options available for addressing the concern. One is to examine the consequences of the postulated failure using the defense in depth evaluation (per BTP-19) to determine whether the existing defense in depth (e.g., other safety or non-safety-related systems, operator actions) gives adequate protection for the design basis events. If this option is selected, results of the defense in depth evaluation would be submitted to the NRC along with a proposed license amendment for review and approval prior to implementing the modification. Another option is to modify the design or make use of alternate designs whose architecture or greater simplicity are such that common cause failure of the system is not a concern. Failure management capabilities may be used to detect and annunciate software-based failures. 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.

---

# 6

## ADDITIONAL GUIDANCE ON ADDRESSING DIGITAL UPGRADE ISSUES

---

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 technical 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.

### 6.1 Background on Digital Quality and Dependability Issues

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 cannot always be detected in design and testing of the system. Software defects can create common mode failures that can defeat the high reliability achieved by use of redundant safety system channels or non-diverse uses of the same software in other systems. Consequently, use of software-based systems introduces concerns regarding the quality of the software and the potential to introduce new modes of failure.

High-quality software and hardware reduces the probability of failure, and this section discusses some of the key elements necessary to provide reasonable assurance that digital systems are of sufficient quality for the intended application. The appropriate level of quality is based on the expertise of the software staff as well as the quality of a design process that incorporates disciplined specification, implementation, verification, validation, and safety analysis. Guidance on digital system design processes is provided in Section 6.3. Part of the design process is specification of appropriate requirements so that the digital equipment is suitable for the intended plant application. Specific digital design and performance issues that should be considered are discussed in Section 6.4. These should be applied to the base platform, tools, and application.

Despite a high quality design, software errors may still 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, 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 analyses is provided in Section 6.5. Section 6.6

describes considerations for demonstrating sufficient dependability such that the risk of failures due to software is acceptably low.

## **6.2 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 grade dedication, and defense-in-depth and diversity analysis include elements of safety significance and complexity.

No quantitative, accepted nuclear standard exists to assess the level of safety significance and the complexity of a digital device. However, some guidance on these subjects is included in the EPRI guideline on use of commercial grade digital equipment (EPRI TR-106439). Regardless of the approach used, when safety significance and complexity are used as a basis for engineering activities, the justification should be documented.

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 (its probability of failure can be set to 0 or 1 with little change), 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 computer science measures of complexity 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.

### **6.3 Digital System Quality**

The design of digital upgrades should place a high importance on quality and reliability. For digital equipment incorporating software, it is well recognized that prerequisites for quality and reliability 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 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 6-1.

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

- ASME NQA-2a, Part 2.7, Quality Assurance Requirements of 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

*Additional Guidance on Addressing Digital Upgrade Issues*

- IEEE 1228, Standard for Software Safety Plans
- IEC 60880, Software for Computers in the Safety Systems of Nuclear Power Stations

**Table 6-1. Industry Software Standards Endorsed by NRC Regulatory Guides**

<b>Regulatory Guide</b>	<b>Endorsed Standard(s)</b>	<b>Scope of Requirements</b>
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, but the more recent versions have not been formally endorsed by the NRC.

### **6.3.1 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 the number of 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. 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 utility 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 must 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.

### **6.3.2 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, 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 which is implemented on a PLC.
- **Configuration data** including software settings that configure a programmable controller and plant-specific setpoints.
- **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 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 must be generated and controlled under a 10 CFR 50, Appendix B quality assurance program.

### **6.3.3 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. V&V 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. 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 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. Independence of V&V activities will increase the odds of finding a problem and dispositioning it properly.

### **6.3.4 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. This is very important for software used in a safety system. 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 effect the rest of the system and are compatible with previously released hardware and software are referred to as “regression” tests.

### **6.3.5 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.

### **6.3.6 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 a process of commercial grade item dedication.

Section 5.3.2 and Annex D of IEEE 7-4.3.2-1993 provides guidance on qualification of existing commercial grade digital equipment. This guidance includes identifying the necessary technical requirements to assure the digital equipment will perform its safety function, and documenting that these characteristics are acceptably implemented.

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 on the safety-significance of the plant application. A supplemental guideline, EPRI TR-107339, also provides useful information and is intended to provide "how to" guidance and examples.

## **6.4 Digital System Design and Performance**

For safety systems in nuclear power plants, the minimum functional design criteria are specified in IEEE 603. 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 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.

### **6.4.1 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 electronics equipment are specified in IEEE 323, and extensive guidance on equipment qualification is provided in EPRI TR-100516, "Nuclear Power Plant Equipment Qualification Reference Manual."

Regarding EMC qualification, EPRI TR-102323 and Regulatory Guide 1.180 provide guidance for addressing the EMC issue for digital upgrades. An important concept in EMC qualification is that equipment can be qualified by (1) site surveys at the point of installation to show the electromagnetic environment is acceptable for the equipment, or (2) testing to show the emissions and susceptibilities of the equipment are acceptable.

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

- Demonstrate that the EMI/RFI levels at which the digital equipment is susceptible will not be credible threats to the equipment as installed.
- Demonstrate that the type of observed susceptibility failures will not adversely affect the safety function of the digital equipment. For example, analog output level oscillations or inaccuracy may not impact the safety-related function or adversely affect plant operation.
- 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.

#### **6.4.2 Human Factors**

The human-system interface includes all interfaces 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 maintenance 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.

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.

### **6.4.3 System Integrity and Failure Management**

The inherent 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 requires that the design of the device include consideration of credible failures and defects and provide features to detect the results of such events. Per IEEE 7-4.3.2, digital equipment must 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 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.

### **6.4.4 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 additional processing time be allowed above the basic system cycle time.

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).

## **6.5 Defense-in-Depth and Diversity**

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

- Control systems;
- Reactor Protection System and Anticipated Transient without Scram;
- Engineered Safety Features; 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 system (RPS and ATWS) are designed to reduce reactivity and shut down the reactor. The engineered safety features (ESF) systems perform 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 RPS or ESFAS, the potential consequences of a common mode 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, NRC expects that an analysis will be performed to assess the vulnerability to common mode failure and demonstrate that adequate diversity and defense-in-depth is available in the overall plant design to cope with such failure. The analysis is performed regardless of the likelihood of failure due to software and as part of the modification process, as shown in Figure 3-1.

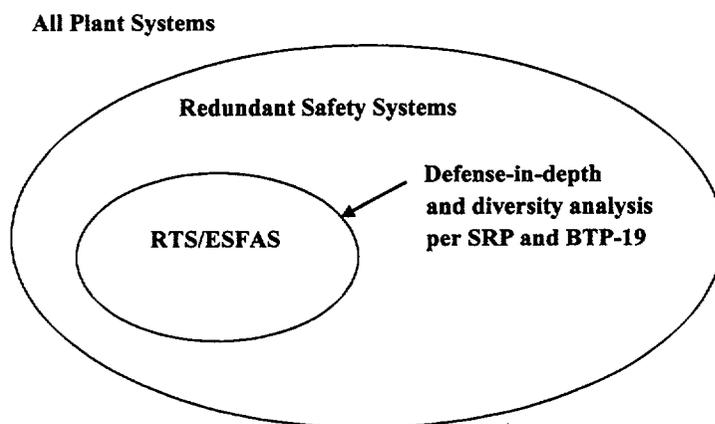
The NRC's expectations for defense-in-depth and diversity analyses are described in BTP HICB 19. The analysis is expected to determine whether safety functions are vulnerable to common mode failure, and if so, to identify diverse manual or automatic means that can perform the same or different functions in order to mitigate design basis accidents and transients. The acceptance criteria in BTP-19 are less restrictive than the plant design criteria in 10 CFR 50 (i.e., the ECCS design criteria in 10 CFR 50.46). Also, re-analysis of design basis events is permitted use "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-19 are considered "beyond design basis" events.

While the BTP 19 analysis is "beyond design basis," the results of the analysis feed into the design and licensing process since they may identify additional diverse functions that should be

added to the system being modified or to other plant systems. Satisfactory compliance with BTP 19 indicates that the potential consequences of common mode failure have been reduced to a level that presents acceptable risk. Failure to satisfy the BTP 19 acceptance criteria may indicate that further design changes are needed to better cope with potential common mode failure.

### **6.5.1 Applicability of Defense-in-Depth and Diversity Requirements**

A formal defense-in-depth and diversity analysis per BTP 19 is only expected for substantial digital replacements of RPS and ESFAS as specified in BTP 19 and Section 7.0-A (e.g., Section C.1, Item 3) of the Standard Review Plan (see Figure 6-1). 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 RPS and ESFAS in IEEE-603 (e.g., Figure 3 of IEEE 603) may also help.



**Figure 6-1. 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-19 is not necessary.

If other I&C systems, including ATWS and other non-safety systems, are being upgraded to digital in plants where digital upgrades to RPS 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 (also see Section 6.5.4).

While the formal defense-in-depth and diversity analysis is only expected for RPS and ESFAS as described above, it is beneficial to consider defense-in-depth in assessing the consequences of any type of potential failures in the failure analysis.

### **6.5.2 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 RPS upgrades at existing plants have used a methodology similar to the following:

- Identify system functions required for protection (RPS) 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.
- 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 is not bounded by the existing analysis, develop engineering rationale justifying that the BTP-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.

### **6.5.3 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.

## **6.6 Dependability and Software Common Mode Failure**

Ultimately, the objective of implementing software quality assurance processes, selecting quality digital devices, and designing robust systems with good failure management is to install a high quality, highly dependable system. To support the licensing process and 10 CFR 50.59 evaluation, a basis for assessing the dependability is needed. For hardware, methods are well established for estimating reliability and probability of failure. However, for software, such quantitative methods do not exist. Without them, some other means is necessary to demonstrate reasonable assurance that the quality of the design is adequate such that the risk of failures, including failures due to software defects, is sufficiently low.

While software reliability cannot yet be quantified, the combination of good engineering practice and proper development, evaluation, and control methods as described in the applicable industry standards and regulatory guidance discussed in the preceding sections can result in high quality digital systems.

Further, thorough failure analysis are used to examine system architecture, design and implementation methodologies, and potential failures with their consequences. Results are fed back into the design process to evaluate the risks of failures and benefits of additional mitigating features. Potential failures due to software are considered as part of prudent engineering in this same fashion, namely on the basis of risk. If the risk of failure, including potential common mode failure, is high enough, prudent design decisions should be made, for example adding limited hardwired controls to perform the design function if necessary.

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:

- Complexity, which can be evaluated as described in Section 6.2. Systems that are sufficiently simple can have well defined potential failure modes and tend to allow for more thorough testing of all input and output combinations than complex systems; conversely, complexity increases the uncertainty associated with demonstrating software quality. The complexity of the digital equipment itself and of the application should be considered.
- The development and quality assurance processes implemented for both the digital platform itself and the plant-specific application software. Ideally, the assessment would demonstrate compliance with appropriate industry standards and regulatory guidelines for development, software safety analysis, failure analysis, V&V, change control, and configuration control as described in the preceding sections. Example 6-1 illustrates this concept.

- Hardware and software design features that contribute to high dependability, such as built-in fault detection and management schemes, internal redundancy and diagnostics, and use of software and hardware architectures designed to minimize failure consequences and facilitate problem diagnosis.
- The maturity of the product and its operating history.
- In-service experience with the platform and the plant system application. Additional confidence is gained if the same equipment and application program have been used successfully in other nuclear plants or other similar applications.

Credit should be taken for using digital platforms that have previously been reviewed by the NRC as part of a generic qualification for safety-related applications. While the effort required on the part of the licensee to evaluate the platform is reduced by the prior NRC review, the licensee will still need to evaluate the plant-specific application. Also, the licensee will need to implement plant-specific action items identified by the NRC as a result of their review.

Aside from software dependability, other issues to consider relating to the overall risk of failure are hardware reliability, compliance with performance requirements for the plant-specific application, and qualification of hardware for the environment.

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, thorough testing may provide reasonable assurance of dependability to compensate for a lack of operating history.

Using the results of this determination and the information developed in the failure analysis, the likelihood and consequences of failure can be assessed using the framework illustrated in Figure 3-2. This approach is illustrated in Example 6-1.

In this example, the digital equipment has been qualified for safety related applications, and has been reviewed by the NRC on a generic basis. This “pre-qualification” reduces the effort required by the utility for the technical evaluation of the platform. The utility would still need to do some additional evaluation, such as reviewing operating history. Also, this example does not discuss the PLC programming tools, but this software (which is not required to be safety-related) would also need to be addressed. It should be covered in the NRC review.

### **Example 6-1. Evaluating Digital System Dependability**

The existing, obsolete load sequencer in each of two redundant ESFAS trains will be replaced using PLCs. The PLCs used in this application have been “pre-qualified” for use in safety-related applications. The load sequencer 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.

Based on a technical evaluation of the PLC platform, it is concluded that the development, V&V, and configuration control of the PLC itself complies with accepted industry standards and regulatory guidance. The design of the system hardware and software includes redundant hardware components for fault tolerance and self-diagnostic features that identify and alarm hardware faults and interruptions in the normal processing routine. A review of operating history shows that the same PLC has been in use for about 5 years in other industries. A FMEA of the PLC system identifies a limited number of possible single failures that are not detected by the system, but that can be detected by application-specific design features. The development processes and hardware qualification have been reviewed by the NRC and found to be acceptable for safety related applications.

The plant-specific application software is very 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 10CFR50, Appendix B QA program in accordance with software life cycle, V&V, and configuration control processes that comply with accepted industry standards and regulatory guidance. An application-specific failure analysis was performed and results were used in the design to reduce the consequences of certain postulated failures.

Additional plant-specific action items identified in the NRC's Safety Evaluation Report on the PLC platform were incorporated in the design as required. 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.

Since the load sequencer is an integral part of the ESFAS system as described in Chapter 7.3 of the UFSAR, a defense-in-depth and diversity analysis was 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-19 acceptance criteria.

As a result of these evaluations, the load sequencer as implemented using the pre-qualified PLC platform is considered to be a high quality, highly dependable system. The risk is considered acceptable, and the change is implemented under 10 CFR 50.59.

# 7

## REFERENCES

---

1. "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants" Code of Federal Regulations Title 10, Part 50, Appendix B.
2. "Changes, Tests and Experiments" Code of Federal Regulations Title 10, Part 50.59.
3. Federal Register Notice, "Changes, Tests, and Experiments," Volume 64, Number 191, Pages 53582-53617, October 4, 1999.
4. NEI 96-07, Revision 1, "Guidelines for 10 CFR 50.59 Implementation," November 2000.
5. NUREG-0700, "Human-System Interface Design Review Guideline," Revision 1, June 1996.
6. NUREG-0711, "Human Factors Engineering Program Review Model," July 1994.
7. NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, Chapter 7," Revision 4, June 1997.
8. NUREG-1709, "Selection of Sample Rate and Computer Wordlength in Digital Instrumentation and Control Systems," June 2000.
9. NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," December 1994.
10. Regulatory Guide 1.22, "Periodic Testing of Protection System Actuation Functions."
11. Regulatory Guide 1.152, Revision 1, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants."
12. Regulatory Guide 1.153, Revision 1, "Criteria for Safety Systems."
13. Regulatory Guide 1.168, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."
14. Regulatory Guide 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

---

*References*

15. Regulatory Guide 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."
16. Regulatory Guide 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."
17. Regulatory Guide 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."
18. Regulatory Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."
19. Regulatory Guide 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis."
20. Regulatory Guide 1.176, "An Approach for Plant-Specific Risk-Informed Decisionmaking: Graded Quality Assurance."
21. Regulatory Guide 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems."
22. Regulatory Guide 1.187, "Guidance for Implementation of 10 CFR 50.59, Changes, Tests, and Experiments."
23. NSAC-105, "Guidelines for Design and Procedure Changes in Nuclear Power Plants."
24. EPRI NP-5652, "Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications."
25. EPRI TR-100516, "Nuclear Power Plant Equipment Qualification Reference Manual," January 1992.
26. EPRI TR-102323, "Guidelines for Electromagnetic Interference Testing in Power Plants," Revision 1, January 1997.
27. EPRI TR-102400, "Handbook for Electromagnetic Compatibility of Digital Equipment in Power Plants," October 1994.
28. EPRI TR-103291, "Handbook for Verification and Validation of Digital Systems."
29. 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.
30. EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," October 1996.

---

*References*

31. EPRI TR-107339, "Evaluating Commercial Digital Equipment for High Integrity Applications: A Supplement to EPRI Report TR-106439," December 1997.
32. EPRI TR-108831, "Requirements Engineering for Digital Upgrades," December 1997.
33. EPRI 1001045, "Guideline on the Use of Pre-Qualified Digital Platforms for Safety and Non-Safety Applications in Nuclear Power Plants," December 2000.
34. NEI White Paper, "Standard Format for Operating License Amendment Requests from Commercial Reactor Licensees," DRAFT, January 19, 2001.
35. IEEE Standard 338-1987, "Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems."
36. IEEE Standard 1012-1998, "Standard for Software Verification and Validation."
37. IEEE Standard 323-1983, "Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations."
38. IEEE Standard 603-1998, "Standard for Criteria for Safety Systems for Nuclear Power Generating Stations."
39. IEEE Standard 7-4.3.2-1993, "Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations."
40. IEEE Standard 1228-1994, "Software Safety Plans."
41. ASME NQA-2a-1990, "Quality Assurance Requirements for Nuclear Facility Applications."
42. IEC 60880, "Software for Computers in the Safety Systems of Nuclear Power Stations."
43. IEC 61508, "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems."
44. ISA-RP67.04.01-2000, "Methodologies for the Determination of Setpoints for Nuclear Safety-Related Instrumentation."