EPRI

Guideline for Performing Defense-in-Depth and Diversity Assessments for Digital Upgrades

Applying Risk-Informed and Deterministic Methods

WARNING:
Please read the Export Control Agreement on the back cover.

Technical Report

Guideline for Performing Defense-in-Depth and Diversity Assessments for Digital Upgrades

Applying Risk-Informed and Deterministic Methods

1002835

Final Report, December 2004

EPRI Project Manager
R. Torok

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

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

ORGANIZATION(S) THAT PREPARED THIS DOCUMENT

Applied Reliability Engineering, Inc.

Électricité de France

MPR Associates, Inc.

Westinghouse Electric Company

EPRI

ORDERING INFORMATION

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

CITATIONS

This report was prepared by EPRI under the guidance of the EPRI/NEI Working Group on Risk-Informed Defense-in-Depth for Digital Upgrades.

EPRI
3412 Hillview Avenue
Palo Alto, California 94304

Principal Investigators
D. Blanchard, Applied Reliability Engineering, Inc.
R. Fink, MPR Associates, Inc.
G. Lang, Consultant
N. Thuy, Électricité de France
R. Torok, EPRI

This report describes research sponsored by EPRI.

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

Guideline for Performing Defense-in-Depth and Diversity Assessments for Digital Upgrades: Applying Risk-Informed and Deterministic Methods, EPRI, Palo Alto, CA: 2004. 1002835.

REPORT SUMMARY

To continue meeting safety and reliability requirements while controlling operating costs, operators of nuclear power plants must be able to replace and upgrade equipment in a cost-effective manner. Instrumentation and control upgrades typically involve either replacement of analog devices with more modern digital technology or updating existing digital equipment. The use of digital technology raises the issue of potential software-related common-cause failure in multiple trains or systems that are safety significant, and the need to ensure that the plant has adequate defense-in-depth and diversity (D3) to cope with such failures. This guide will help nuclear plant operators address D3 issues in a consistent, comprehensive manner.

Background

In response to growing challenges of obsolescence and increasing maintenance costs – and now looking ahead to license renewal – nuclear plant operators are upgrading their existing instrumentation and control (I&C) systems. Preferred upgrade solutions typically apply digital technology due to its ready availability, operational flexibility, and potential for performance and reliability improvements. However, the use of digital equipment has raised technical and licensing issues, primarily centered on the potential for new behaviors and failure modes caused by software or other digital system design flaws. Of particular concern is the potential for common-cause failures, which disable multiple equipment trains or systems that use identical software-based components. Current regulatory guidance recommends that a D3 evaluation be performed for selected upgrades to confirm that the plant has adequate coping capability for digital system common-cause failures. This largely deterministic approach sometimes results in significant utility and Nuclear Regulatory Commission (NRC) resources spent on events, components, and backup systems that do not 1) contribute significantly to plant risk, 2) address other events that may be significant contributors, and 3) improve plant safety. The industry needed a D3 approach for digital upgrades that would maintain a better focus on plant safety, while ensuring any backups added provide value in terms of plant safety or risk.

Objective

To help plant operators perform D3 evaluations for digital upgrades in a systematic, technically sound manner, with a focus on maintaining plant safety.

Approach

An EPRI working group comprised of utility and industry representatives oversaw development of the guideline. The basic approach was to extend current D3 regulatory guidance for digital upgrades to include use of risk-informed insights, consistent with regulatory guidance on use of the probabilistic risk assessment (PRA). At present, there are no consensus methods for precisely estimating probabilities of failure for software-based equipment. The guideline takes the position

that qualitative techniques can be used to make estimates that are adequate to extract the risk insights needed for D3 evaluations.

Results

This guide helps plant operators design and implement digital upgrades, perform D3 evaluations, and develop information to support licensing submittals. Three methods for D3 evaluation are presented as alternatives to the current deterministic approach: an "extended deterministic" method based on the current approach; a "standard risk-informed" method based on use of the PRA as modified to reflect the digital upgrade; and a "simplified risk-informed" method that uses data from the existing, unmodified PRA. Users will be able to select the most appropriate method on a case-by-case basis. This document also provides guidance on using digital system design, development process, and operating history attributes to assign digital system failure probabilities for PRA analysis, with examples outlining the evaluation steps. This will be helpful to analysts in updating PRA models to reflect digital upgrades. Where possible, the guideline provides a road map to relevant standards and other sources of detailed guidance.

EPRI Perspective

This project is part of a multi-year EPRI initiative to help plant operators design, implement, and license digital I&C upgrades in nuclear power plants. This guideline is particularly significant in that it provides a practical approach for the difficult issues of D3 evaluation and PRA modeling for software-based equipment. The risk-informed framework here is unique in that it considers not only the potential adverse behaviors of digital equipment in risk-significant applications, but also the characteristics and features of the new technology that lead to improvements in safety. Methods for modeling digital equipment in the PRA, and particularly for determining failure probabilities, are still evolving. However, the framework proposed here should remain valid and useful as more precise methods become available. In the meantime, the methods proposed here represent a significant improvement over the simple, but overly restrictive assumption that software common-cause failure happens with certainty.

Both the industry and the NRC staff have recognized the potential for enhanced safety and reliability that digital systems bring to the nuclear industry. However, uncertainties in the licensing treatment of D3 for digital upgrades have led several plant operators to postpone planned upgrades. With the great majority of plants now anticipating license renewal and decades of continued operation, the need to replace aging I&C systems has become more obvious and more acute. A consensus approach between regulators and licensees is therefore needed to ensure that the treatment of digital technology-related issues is predictable and consistent. EPRI anticipates that this guideline on D3 evaluations for digital upgrades will receive endorsement and wide usage by the nuclear power industry.

Keywords

Instrumentation and Control
Digital Upgrade
Common-Cause Failure
Common-Mode Failure
Defense-in-Depth

ACKNOWLEDGMENTS

The development of this guideline was led by the EPRI/NEI Working Group on Risk-Informed Defense-in-Depth for Digital Upgrades. The membership is shown below:

Jack Stringfellow	Southern Nuclear	Co-chairman
Steve Swanson	Southern Nuclear	Co-chairman
Jay Amin	TXU Power	
Jim Andrachek	Westinghouse Electric Company	
Paul Bisges	AmerenUE	
Dave Blanchard	Applied Reliability	
Jay Bryan	Duke Energy	
Bob Contratto	NUC-DCS Integrators	
Ray Disandro	Exelon Nuclear	
Larry Erin	Westinghouse Electric Company	
Bob Fink	MPR Associates, Inc.	
John Hefler	Altran	
Tim Hurst	Hurst Technology	
Ron Jarrett	TVA	
Glenn Lang	Consultant	
Phil Liddle	Framatome ANP	
Peter Lobner	DS-S	
Rich Luckett	NEI	
Jerry Mauck	Framatome ANP	
Jim Mcquighan	Calvert Cliffs	
Nguyen Thuy	EPRI, EdF	
Denny Popp	Westinghouse Electric Company	
Clayton Scott	Triconex	
Bill Sotos	STP	
Andrea Sterdis	Westinghouse Electric Company	
Jeff Stone	Calvert Cliffs	
Dinesh Taneja	Bechtel	
Dan Tirsun	TXU Power	
Ray Torok	EPRI	
Philip Wengloski	Calvert Cliffs	

Also, the Working Group wishes to acknowledge the contribution of many individuals in the industry who reviewed and commented on drafts of the guideline. The suggestions and comments they provided have been extremely helpful in developing a workable approach for evaluating defense-in-depth and diversity of digital upgrades.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1
INTRODUCTION

1.1 Objective

This document provides guidance to support utilities in performing defense-in-depth and diversity (D3) evaluations associated with digital upgrades that affect plant instrumentation and control (I&C) systems. For some digital upgrades, a D3 evaluation is performed to examine potential vulnerability to software or other digital system failures that could simultaneously affect multiple trains or systems. Such failures are referred to in this report as digital common cause failures (digital CCFs)[1]. The focus of a D3 evaluation is on digital CCFs that could degrade plant safety. Postulated digital CCFs could compromise the redundancy built into safety systems, or impact defense-in-depth currently provided through the availability of independent protection, control and monitoring systems.

Guidance is provided for determining when a D3 evaluation is necessary, identifying susceptibilities to digital failures and digital CCFs, evaluating resulting plant vulnerability, and determining the need for additional defense. The methods presented combine deterministic and risk-informed techniques. Use of risk insights can help focus the D3 effort on areas of greatest potential benefit in terms of plant safety. It also allows credit to be taken for the positive impacts of modern digital equipment on system reliability and safety. Finally, it can help justify not adding backup systems that do not provide benefit in controlling plant risk.

The guidance in this document was produced by an industry Working Group including personnel from plants' I&C and Probabilistic Risk Assessment (PRA) groups, equipment suppliers, and consultants. It is intended for use by plant engineering, licensing and management personnel who need to gain a basic understanding of the D3 issue and make informed decisions about how it will be addressed when making digital upgrades. These decisions include determining when a D3 evaluation should be performed, what method should be used, important considerations in applying the method, and who should be involved in doing the evaluation (I&C designers, PRA analysts, etc.). System suppliers or contractors involved in performing D3 evaluations also can use this guidance.

[1] These failures are often referred to as "software common mode failures" in other documents. We use digital common cause failure (digital CCF) in this document to more accurately describe the types of failures that are of concern. They result in a deterministic and systematic manner from design errors, which may occur in developing the requirements, the design, or the implementation (e.g., coding) of the software or the hardware-software (digital) system. They are common cause in that multiple pieces of equipment fail due to a single cause (the design flaw).

1.2 Background

Nuclear utilities are now replacing and upgrading aging and obsolete I&C systems. Most of these replacements involve transitions from analog to digital technology, which has evolved since the plants were designed and built. Digital systems offer the potential to improve plant safety and reliability through features such as increased hardware reliability and stability, improved failure detection capability, and enhanced controls algorithms. Still, because of increased complexity and the relative newness of the technology to nuclear plants, the use of digital equipment has raised technical and licensing issues. These are centered on the potential for new behaviors and failure modes due to software or other digital system design flaws (hereafter referred to as "digital faults").

Various development practices and standards are applied that help ensure digital safety systems are of high quality (e.g., see References [3], [18], [22], [26]). However, in most cases, the potential exists that a failure due to a postulated digital flaw could disable redundant trains or backup systems that use identical design elements (e.g., software modules, digital components, or functional specification elements).

To help establish reasonable assurance that digital failures will not lead to unacceptable results, the current regulatory guidance for digital upgrades (Branch Technical Position HICB-19, referred to as BTP-19, (see Reference [1]) recommends that a D3 evaluation be performed for digital upgrades to the reactor trip system (RTS) or the engineered safety features actuation system (ESFAS). The purpose of the evaluation is to confirm that in the event of a digital CCF, the plant has sufficient "coping" capability such that the plant response will be acceptable. This evaluation is considered beyond design-basis, and as a result may use best-estimate assumptions and techniques and take credit for non-safety systems, provided they are of sufficient quality.

The NRC position concerning D3 evaluations is documented in BTP-19 and NUREG/CR-6303 (see Reference [5]). Although it contains some risk-informed elements, the approach recommended is largely deterministic. Experience in applying it to actual plant upgrades, and scoping studies performed by EPRI to examine risk insights offered by PRAs (see Reference [20]), have identified a number of shortcomings. In particular, it often results in significant effort being spent by the licensee and NRC on events that do not contribute significantly to plant risk. At the same time, it does not address other events that may be significant contributors to risk, as indicated by the plant PRA.

The NRC has also published a policy statement (see Reference [24]) that encourages use of PRA in a variety of regulatory activities, and guidelines on the use of PRA for licensing basis applications (Regulatory Guide 1.174, see Reference [2]). These have established a foundation upon which risk-informed approaches can be applied to D3 evaluations. Use of such approaches can help focus the D3 effort on the areas of greatest potential benefit in terms of plant risk, and avoid addition of unnecessary backups that add complexity but do not contribute to improving plant safety. Since BTP-19 was published, all nuclear power plants in the U.S. have completed plant-specific PRAs.

1.3 Scope

- This document provides guidance for:
- Determining if a digital upgrade project should undergo a D3 evaluation.
- Identifying susceptibilities to digital failures and digital CCFs that should be addressed in the D3 evaluation.
- Performing the D3 evaluation, using methods that combine deterministic and risk-informed techniques.
- Meeting regulatory requirements and expectations for D3 evaluations.
- Documenting the evaluation and the results.

The guidance is intended to apply to the full range of digital upgrades, from individual component replacements to large-scale conversions of I&C systems to digital equipment. It also covers "digital-to-digital" changes, i.e., changes to, or replacement of, existing digital equipment. It can be used to help determine an appropriate I&C architecture from the standpoint of maintaining defense-in-depth and managing risk associated with digital equipment, to update the plant PRA to reflect the upgrade, and to assess the impact on plant risk.

The following principles and ground rules have been established by the industry Working Group:

- For performing D3 evaluations, plants should be able to use any method that can be shown to meet the original intent of BTP-19 (see Reference [1]) (that is, that adequately addresses vulnerabilities to digital CCFs). This may include deterministic methods, risk-informed methods, and methods that blend the two approaches.
- Addition of backups to address digital CCFs should be approached judiciously. Adding new equipment can increase system complexity, probability of spurious trips/actuations, maintenance and training burden, and thus can have a negative impact on plant safety. Risk assessments should include consideration of risk associated with additional backups.
- At present there are no consensus methods for precisely quantifying the impact of potential digital faults on the reliability of digital equipment. However, qualitative assessment techniques can be applied to form judgments regarding the impact of digital equipment on overall system reliability and plant risk.
- Assessments of the contribution of digital equipment to plant risk should recognize that not all digital faults lead to unsafe system failure. Risk assessments should consider the design of the digital equipment and the conditions under which it will be operating when assessing the contribution to plant risk.
- Assessment of risk should consider positive impacts of digital equipment on system reliability and plant risk, including factors such as increased hardware reliability, redundancy, and failure detection.

These principles are consistent with NRC's approach for using risk insights in the licensing process. Shifting D3 evaluation to more risk-informed approaches is directly supportive of Commission policies on risk-informed applications and reduction in unnecessary regulatory burden. As stated in Regulatory Guide 1.174 (see Reference [2]), it is *"…NRC's desire to base its decisions on the results of traditional engineering evaluations, supported by insights (derived from the use of PRA methods) about the risk significance of the proposed changes. Decisions concerning proposed changes are expected to be reached in an integrated fashion, considering traditional engineering and risk information, and may be based on qualitative factors as well as quantitative analyses and information."*

1.4 Relationship to Other Documents

This guideline supplements the following related industry and regulatory guidance documents and should be used along with these documents when performing D3 evaluations:

- **EPRI TR-102348 Revision 1 (NEI 01-01)** (see Reference [3]) – This is the industry guideline on licensing of digital upgrades. It describes how digital upgrades and the associated licensing issues can be addressed in the modification design process and in 10 CFR 50.59 (see Reference [9]) evaluations. It also provides high-level guidance on dealing with the issue of digital CCFs. TR-102348 Revision 1 was endorsed by the NRC in Regulatory Issue Summary 2002-22 (see Reference [4]). The guidance given here is consistent with and supplements the guidance in TR-102348 Revision 1, specifically in the area of D3 evaluation and use of risk insights in performing the evaluation.
- **BTP-19** (see Reference [1]) – This Branch Technical Position, in Chapter 7 of the Standard Review Plan (NUREG-0800, see Reference [14]), describes the NRC position on defense-in-depth and diversity, describes an acceptable method for performing D3 evaluations, and specifies acceptance criteria. The approaches described in this report meet the intent of BTP-19 in addressing vulnerabilities to digital CCFs.
- **NUREG/CR-6303** (see Reference [5]) – This NRC contractor report describes in detail the method for performing D3 evaluations that is referenced in BTP-19. It also includes guidance for determining whether there is sufficient diversity between different portions of a digital system such that they would not be subject to the same digital CCF. Section 3.1 of this report presents an updated approach that extends the NUREG/CR-6303 guidance to include consideration of digital design features and defensive measures that impact the potential for CCF and to incorporate the use of risk-informed insights.
- **Regulatory Guide 1.174, Revision 1** (see Reference [2]) – This NRC regulatory guide describes a method acceptable to the Staff for using risk-informed approaches and the plant PRA to support changes to the licensing basis. The guidance provided in this report makes use of the approach and criteria described in Regulatory Guide 1.174 to support application of risk insights when performing D3 evaluations.

1.5 Contents of This Guideline

Section 2 of this document describes the current regulatory context for D3 evaluations, and then presents a risk perspective on D3, including the primary factors that should be considered in assessing the impact of digital upgrades on plant risk.

Section 3 provides overall guidance on performing D3 evaluations, covering the evaluation process, what should be considered in identifying specific susceptibilities to digital failures and digital CCFs that need to be addressed, and three methods for performing the D3 evaluation. The three methods represent alternatives to the method described in BTP-19 (see Reference [1]).

Section 4 provides additional guidance to support utilities in performing D3 evaluations. This includes more detail on digital equipment characteristics that could be examined when assessing susceptibility to digital failures and digital CCFs, basic principles of risk-informed analysis, and level of detail involved in modeling digital equipment in the PRA. Section 4 also provides guidance on documenting the D3 evaluation.

2
D3 EVALUATION – REGULATORY CONTEXT AND RISK-INFORMED PERSPECTIVE

For the purposes of this guideline, a defense-in-depth and diversity (D3) evaluation is:

- An assessment of the susceptibility of the plant systems to digital failures and digital CCFs, and
- An evaluation to determine whether the plant has sufficient coping capability to adequately deal with such failures in terms of their effects on plant safety.

This section describes the regulatory context for deterministic D3 evaluations and identifies shortcomings of the approach described by current regulatory guidance. It then presents a risk-informed perspective on D3 evaluations, discussing the regulatory context, the impact of digital upgrades on plant risk, and how the use of risk-informed techniques can address the identified shortcomings.

2.1 Regulatory Context – Deterministic Approach

2.1.1 Current Regulatory Guidance

The NRC has expressed the concern that software design errors are a credible source of CCFs (see References [1], [7]) that could degrade the existing defense-in-depth provided by the four echelons of defense: control systems, RTS, ESFAS, and monitoring and indications. Its position to address this concern is stated in four points in BTP-19 (see Reference [1]):

1. *The applicant/licensee should assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-mode failures have been adequately addressed.*
2. *In performing the assessment, the vendor or applicant/licensee shall analyze each postulated common-mode failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best-estimate methods. The vendor or applicant/licensee shall demonstrate adequate diversity within the design for each of these events.*
3. *If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, should be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.*

4. *A set of displays and controls located in the main control room should be provided for manual system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls should be independent and diverse from the safety computer systems identified in items 1 and 3 above.*

All four points apply to advanced reactors. Points 1, 2 and 3 apply whenever an operating plant replaces its existing (typically analog or relay-based) RTS or ESFAS with a digital system. NUREG/CR-6303 (see Reference [5]) provides detailed guidance for performing a D3 evaluation using a method (hereafter called the BTP-19 Deterministic Method) that the NRC has determined is acceptable.

D3 evaluations are "beyond design-basis" (SECY-93-087, see Reference [7]). Therefore, they can be performed on a "best-estimate" basis. Thus, realistic initial conditions and assumptions can be used, as opposed to the conservative assumptions applied in the plant licensing basis safety analysis. This concept is also discussed in EPRI TR-102348 Revision 1 (NEI 01-01) (see Reference [3]).

2.1.2 Relationship to 10 CFR 50.59 Evaluations

The 10 CFR 50.59 regulation (see Reference [9]) specifies the criteria for determining whether a license amendment is needed before implementing a plant modification. As discussed in EPRI TR-102348 Revision 1 and NEI 96-07 Revision 1 (see Reference [15]), the only failures that need special consideration and NRC review based on a 10 CFR 50.59 evaluation are those that are as likely as the failures already considered in the plant's licensing basis (as described in the SAR).

For equipment that has been evaluated for safety applications, the likelihood of digital CCF should be well below the likelihood of random single failures assumed in the licensing basis. Therefore, although the potential for digital CCFs should be considered in the evaluation, it typically would not by itself lead to the need for a license amendment per 10 CFR 50.59.

Digital CCFs and their potential D3 issues should be addressed in the design process for the modification (independent of the 10 CFR 50.59 evaluation). Information on the digital equipment design, qualification and application should be examined to ensure that the likelihood of digital CCF is much lower than the likelihood of random single failures assumed in the licensing basis.

2.1.3 When a D3 Evaluation is Needed (Regulatory Perspective)

D3 evaluations are not required for all digital upgrades, based on the existing regulatory guidance. According to the Standard Review Plan (SRP) presented in Chapter 7, Section 7.0A of NUREG-0800 (see Reference [14]), NRC expects a D3 evaluation to be performed for digital upgrades "*…that involve a reactor trip system (RTS) or an engineered safety features actuation system (ESFAS)…*" The SRP further states that D3 evaluations should be performed specifically for "*I&C safety systems incorporating digital computer technology…*" within RTS or ESFAS.

This was reiterated in Section 5.2.1 of EPRI TR-102348 Revision 1 (see Reference [3]), which states that "*A formal defense-in-depth and diversity analysis per BTP/HICB-19 is expected only for substantial digital replacements of RTS and ESFAS …*" It also points out that it is sometimes not clear whether a system should be considered as part of ESFAS. TR-102348 Revision 1

recommends when in doubt, to review the SAR to determine how the system is described there (e.g., is it described as part of ESFAS in Section 7.3 of Chapter 7, or as an auxiliary system in Chapter 9?). The definitions of RTS and ESFAS in IEEE-603 (see Reference [21]) also may help with this determination. Note that human-system interfaces that are required to perform any human actions credited in the SAR are part of the RTS or ESFAS.

As also discussed in TR-102348 Revision 1, cumulative effects of a series of upgrades or modifications should be considered when determining whether a D3 evaluation should be performed. Consideration should be given to the effects the change(s) may have collectively on defense-in-depth and diversity of the RTS/ESFAS functions.

Example 2-1. Cumulative Effects of a Series of Upgrades.

Digital technology is to be introduced into plant systems, including anticipated transient without scram (ATWS) and other non-safety systems, after a digital upgrade to RTS or ESFAS has already been implemented (and a D3 evaluation performed at that time). If equipment being modified was credited as a backup in the prior D3 evaluation, then the evaluation should be reviewed to determine the impact of the current modification. The review should determine whether the proposed change might invalidate the conclusions of the evaluation, and thus require additional mitigation measures.

Note that a "digital-to-digital" change to RTS or ESFAS also may involve review of a previous D3 evaluation. If the change may affect the conclusions of the evaluation, then it should be reviewed and updated as necessary to ensure the conclusions are still valid.

The flowchart of Figure 2-1 illustrates the process for determining whether a new D3 evaluation should be performed, or a previous evaluation reviewed as a result of a planned modification.

2.1.4 Weaknesses of the BTP-19 Deterministic Method

Plants and vendors who have attempted to apply the BTP-19 (see Reference [1]) Deterministic Method for D3 evaluations have encountered difficulties and identified a number of shortcomings:

- The method addresses only the initiating events analyzed in the plant SAR, but not all the initiating events evaluated in the plant PRA. Consequently, it may not address significant contributors to risk.
- Significant effort may be required to analyze each initiating event in the plant SAR using best-estimate assumptions and initial conditions.
- The SAR events are treated as though all are equally safety-significant, and diverse backups are considered equally valuable for all events / systems. There is only limited recognition that the risk associated with these events may vary depending on the frequency of the event, and no recognition that that risk varies with the probability of failure of the mitigating systems. Meeting the acceptance criteria for some events may require the addition of diverse mitigating functions, even when the events are insignificant contributors to risk in the plant PRA.

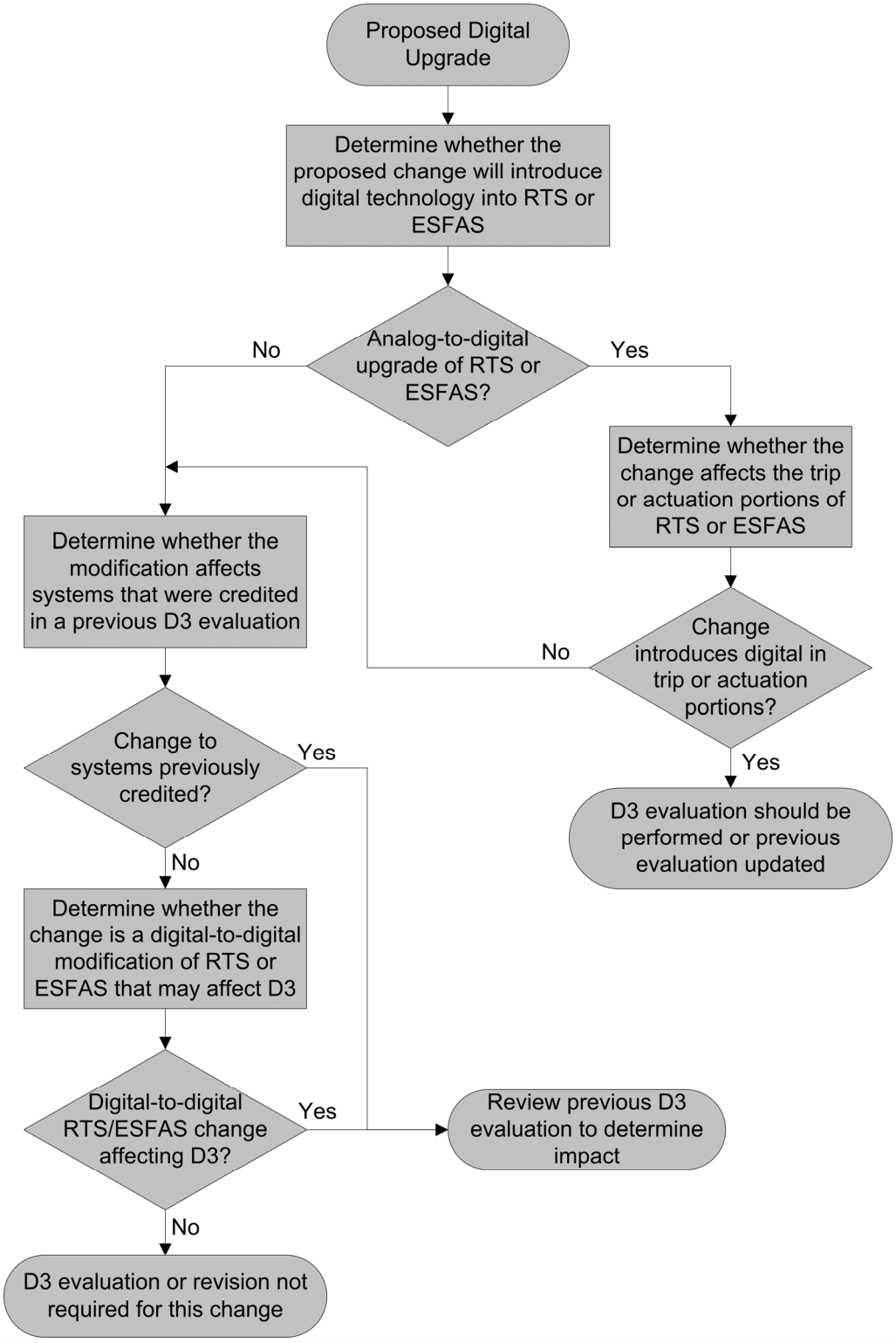

Figure 2-1
Determining When a D3 Evaluation is Needed (Regulatory Perspective)

- The postulated digital CCFs are assumed either to occur or not to occur (i.e., their probabilities are either 1 or 0), yielding either a very conservative result or a potentially non-conservative result. The method does not allow for examination of digital equipment design features and other defensive measures that could justify digital CCF probabilities between 0 and 1.
- The method does not allow the analyst to factor into the evaluation the positive impacts of digital equipment on reliability of the mitigating systems. For example, no credit is taken if the new equipment adds internal redundancy, or the ability to detect faults in the I&C or other parts of the system.

Example 2-2. Risk Insights on Large Break LOCA.

Typically, for D3 evaluations performed per BTP-19 and NUREG/CR-6303 (see Reference [5]), meeting the acceptance criteria for the large break loss of coolant accident (LBLOCA) event has proven to be difficult when a concurrent digital CCF is assumed, even using best-estimate assumptions. One option to satisfy the BTP-19 acceptance criteria would be to install a diverse mitigation function, but this would require additional analysis, equipment and maintenance. The use of risk insights might show that LBLOCA is a very small contributor to plant risk and that adding such equipment might actually increase risk by adding new failure modes. However, application of risk insights might also show that some high-frequency initiating events that are acceptable per the BTP-19 acceptance criteria are potentially risk-significant and deserve greater attention.

2.2 Risk-Informed Perspective

2.2.1 Current Regulatory Guidance

In Generic Letter 88-20 (see Reference [23]), the NRC requested all licensees to perform Individual Plant Evaluations (IPEs) to assess the vulnerability of the plant designs to severe accident risks. Performance of a detailed plant-specific PRA was encouraged by the NRC in completing the IPE requirement. Among the various benefits identified, a PRA was considered useful in its support of licensing actions, including the evaluation of design modifications to the plant.

Subsequent to Generic Letter 88-20, the NRC published the PRA policy statement (see Reference [24]), in which the Commissioners stated that:

- Because PRA considers the frequency of a broad spectrum of initiating events and combines them with an assessment of the reliability of mitigating systems, including the potential for multiple and common cause failures, it is considered an extension and enhancement of traditional regulation.
- PRA techniques are most valuable when they serve to focus the traditional deterministic-based regulations and support the defense-in-depth philosophy.

- The PRA approach supports the NRC's defense-in-depth philosophy by allowing quantification of the levels of protection, and by helping to identify and address weaknesses or overly conservative regulatory requirements applicable to the nuclear industry.

Consistent with these assertions, the Commissioners instructed the NRC and encouraged the industry to increase the use of PRA:

- In all regulatory matters, to the extent supported by the state-of-the art in PRA methods and data, and in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy.
- In regulatory matters, where practical within the bounds of the state-of-the-art, to reduce unnecessary conservatism associated with current regulatory requirements, regulatory guides, license commitments, and NRC practices.

When BTP-19 (see Reference [1]) was issued, plants had not yet developed their PRAs. However, all plants have now completed them. By taking advantage of information available in the plant PRA, this guideline both enhances and focuses existing regulatory guidance regarding evaluation of the plant capability to cope with digital failures.

To be considered risk-informed, analysis of changes to the licensing basis should meet a key set of principles and criteria, as outlined in Regulatory Guide 1.174 (see Reference [2]). (See Section 4.3 for a discussion of these principles and their relationship to D3 evaluation.) The D3 evaluation methods presented in this guideline meet the principles and criteria outlined in the Regulatory Guide, and therefore are considered to be risk-informed.

2.2.2 Contribution of Digital Upgrades to Plant Risk

From a risk-informed perspective, the digital equipment and its postulated failures are only a part of a larger picture. There are three factors that determine the impact of a digital upgrade on plant risk:

Factor A: Impact of the upgrade on I&C channel reliability.

Factor B: Potential for digital CCF introduced by the upgrade.

Factor C: The design of the plant and the plant mitigating systems available to respond to specific events affected by the upgrade (sometimes called the plant safety model).

It is the combined effects of these factors that determine impact on plant risk. Strength in one factor may compensate for weakness in another. Their relative levels of importance can vary with application specifics, and considering only one of them can lead the analyst to over estimate its relative importance. The BTP-19 Deterministic Method is significantly limited in that it focuses primarily on factor B, applying conservative, bounding (potentially misleading) assumptions. Factor A is largely ignored, and only parts of factor C are addressed, through best-estimate evaluation of the SAR events.

Note that susceptibility to digital CCFs is not the same as plant risk or safety vulnerability. It is possible to introduce susceptibilities to digital CCFs that have negligible impact on plant risk, depending on the influence of factor C above. The potential digital CCFs of importance are those that have significant adverse impact on plant risk. A brief discussion of each of these three factors follows.

Factor A. Impact of the Upgrade on I&C Channel Reliability

This factor relates to the impact of the digital upgrade on reliability (or the complementary concept, probability of failure (P_F)) of individual channels of I&C equipment.

It is important to note that just because there are "bugs" in the software or flaws in the design does not necessarily mean that there will be digital failures. The likelihood of digital failure within an I&C channel depends on the number of digital faults remaining after development and verification, **and** on the likelihood that:

- An unanticipated operational condition will occur that activates a fault.
- This activation causes a failure (some activations lead to non-optimal but still acceptable results, or are overridden before they can have any functional consequences).

It is also important to note that not all channel failures have potential consequences on risk. Some do not affect safety functions, do not create hazardous conditions, or occur only in contexts where they have no effect on safety. In this guideline, implicitly, only the potentially risk-significant failures are considered, and "failure" stands for "potentially risk-significant failure". These may be divided into two categories:

- Potentially unsafe failures are failures that could prevent a mitigating function from occurring when needed.
- Potentially initiating failures are failures that could trigger an initiating event (e.g., failure of a control loop in a direction that could cause a transient that challenges the safety systems).

A digital upgrade may introduce internal redundancy and self-checking into single channels of the system, which could significantly improve channel reliability. However, if such features add too much complexity, this could increase the potential for digital failure.

Factor B. Potential for Digital CCF

The second factor relates to whether digital failures become CCFs that affect multiple channels or multiple systems. The independence criterion of IEEE 603 (see Reference [21]) provides reasonable assurance that failures will not propagate from one channel or system to another. If it is satisfied, a digital failure of a channel can become an intra-system CCF only when the activating condition concurrently affects other redundant, identical channels. A digital CCF affecting two digital systems concurrently would depend on a number of additional conditions:

- The activating condition that triggered digital failure of the first system also affects redundant channels of, and was unanticipated in, the second system.

- The design of the second system is such that the condition activates the same or a causally related digital fault, resulting in a failure.
- The function of the second system is such that this failure could prevent necessary mitigation or trigger an initiating event.

Figure 2-2 illustrates the conditions required for a digital fault to result in a failure of an I&C channel (Factor A), the additional conditions required for it to affect redundant channels within a system, and the conditions necessary for it to affect a second system (Factor B).

Diversity, or differences in key elements of software and hardware processes and components, is one means of limiting the susceptibility to digital CCF, as described in NUREG/CR-6303 (see Reference [5]). Other types of defensive measures in the design of an upgrade also can help reduce the likelihood of digital CCF, even when identical hardware and software components are used in multiple channels or systems. Section 3.1 discusses evaluation of defensive measures as part of determining whether a digital upgrade may introduce susceptibilities that should be addressed in the D3 evaluation.

Factor C. Plant Design / Safety Model

The risk impact of digital failures and digital CCFs (factors A and B) depends in part on what initiating events are affected, and on the design of the systems available to respond to those events. Assessment of plant risk therefore involves consideration of the intrinsic level of D3 in the plant design. This is defined predominantly by the combination of the mechanical and electrical mitigating systems available to respond to the relevant initiating events.

Figure 2-3 shows an example of how the various elements of the plant design and safety model contribute to risk for a given initiating event. For each event, there are one or more functions that can provide mitigation and prevent core damage. These functions may be performed by safety or non-safety related systems, and may include manual operator actions. Some systems may have internal redundancy while others have only a single train of equipment. Note that the alternate mitigating systems shown in the figure include both digital and mechanical/electrical equipment needed to perform the function. The options of using operator action or an additional (diverse) automatic actuation capability represent alternate ways of backing up the I&C of the mitigating system.

Combining Factors A, B and C

The impact of a digital upgrade on a given initiating event's contribution to risk is determined by:

- The impact of the upgrade on the initiating event frequency (F_{IE}). While often dominated by hardware failures, factors A and B could influence the frequency of the initiating events for which I&C failures play a role, if they substantially change the reliability of the I&C or of the key hardware components.
- The impact on reliability (or failure probability) of the digital components of a single mitigating system, including:

  - The probability of potentially unsafe digital failure (P_{DF}) of individual I&C channels (factor A).
  - The likelihood of a potentially unsafe digital CCF affecting redundant I&C channels. This is represented in PRAs by a "beta-factor" (factor B).
  - The probability of failure (P_F) of any digital equipment, signals, logic, etc., that is not redundant in the system (factor A for digital failures, plus random hardware failures).
- The availability of multiple mitigating functions (factor C), possibly including operator action and/or new mitigating functions, and the potential for inter-system digital CCF that could affect multiple mitigating functions (factor B).
- The likelihood of a digital CCF that could affect the initiating event and a mitigating system concurrently (i.e., causing the event and at the same time preventing a mitigating system from operating, with an associated beta-factor for this CCF).

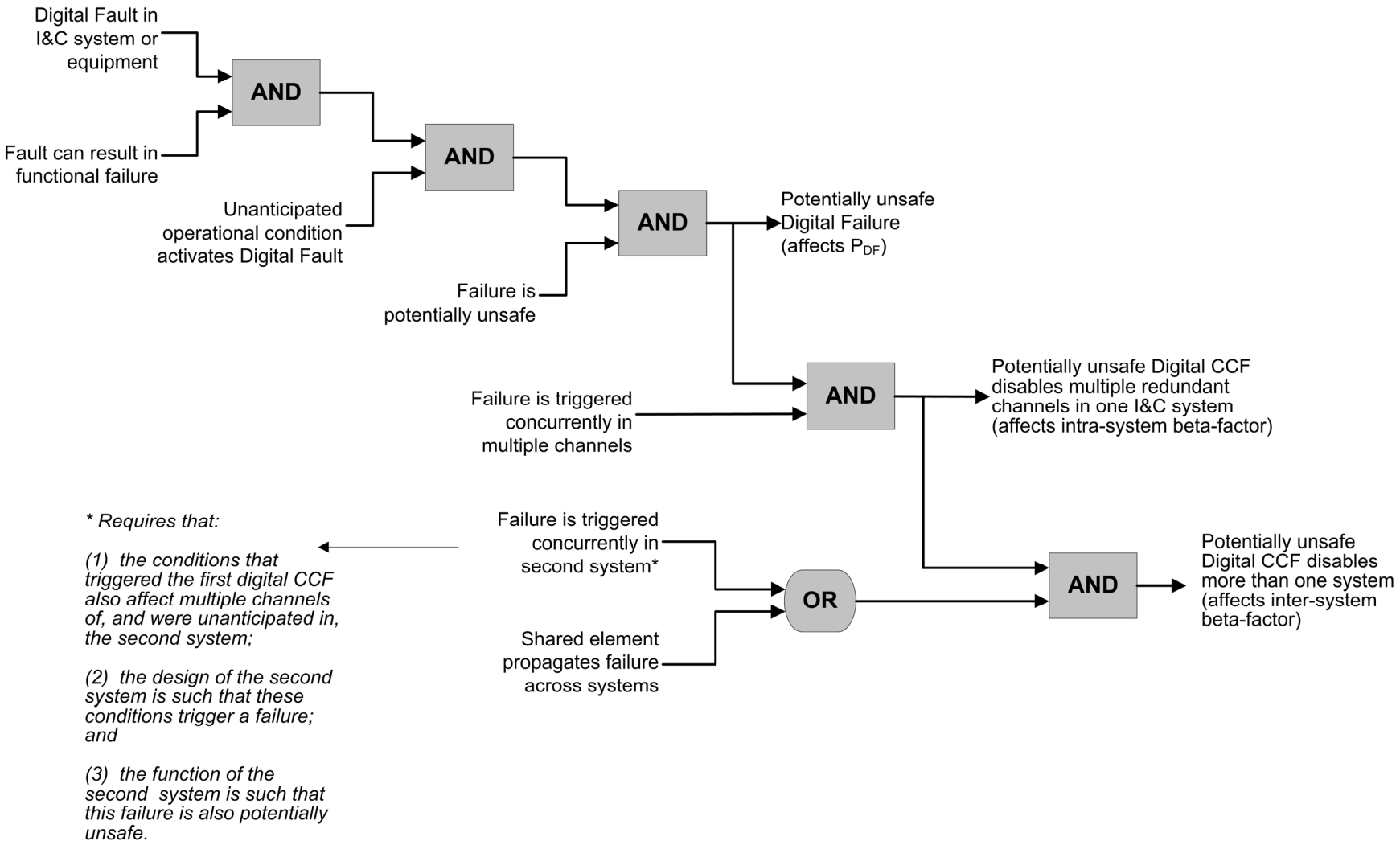

Figure 2-2
Conditions That Must be Present for a System to be Susceptible to Potentially Unsafe Digital Failure (Factor A) and Digital CCF (Factor B)

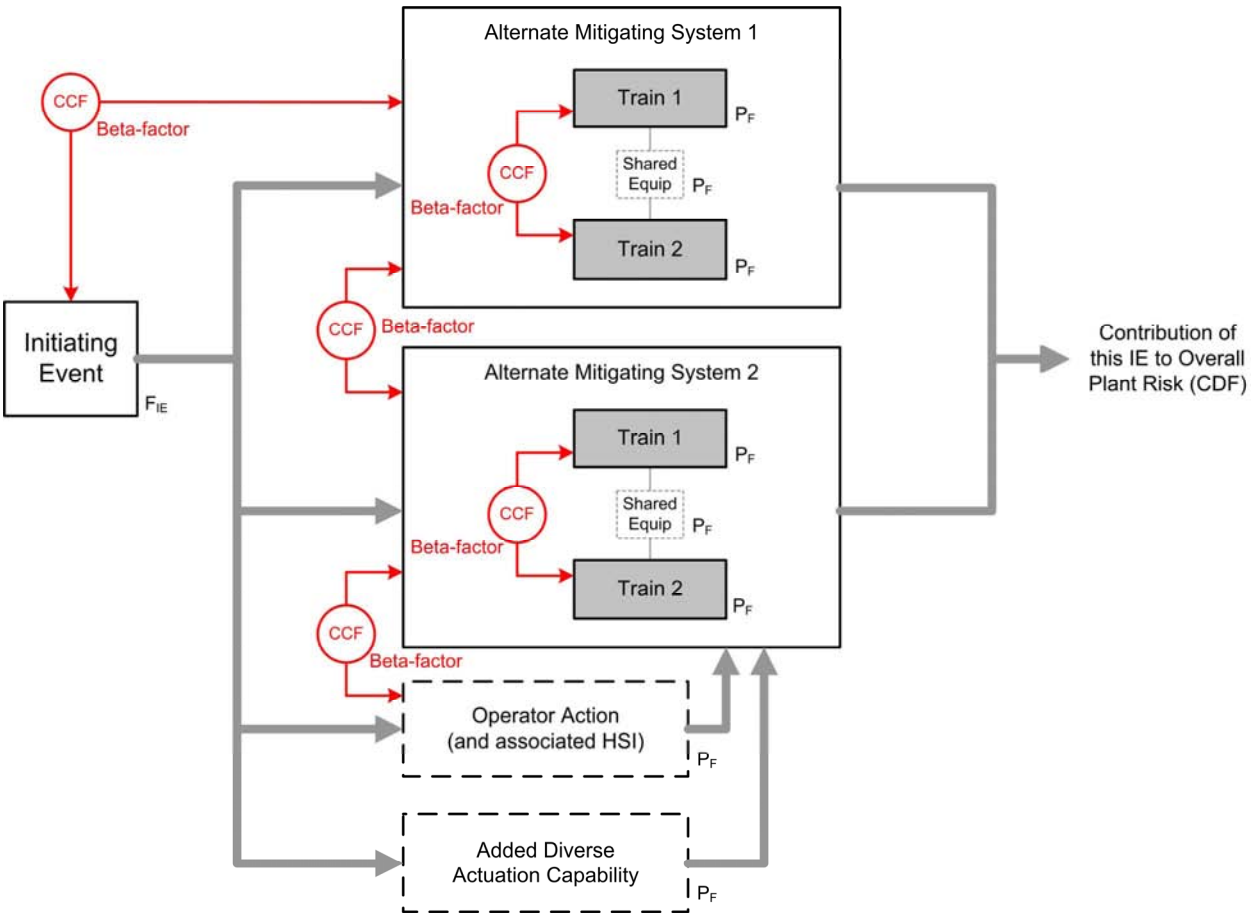

Figure 2-3
Effects of Plant Design / Safety Model (Factor C) on Risk Associated with a Digital Failure

2.2.3 When to Perform a D3 Evaluation (Risk-Informed Perspective)

Evaluation of the potential failure modes and risks associated with digital upgrades should be performed regardless of whether a formal D3 evaluation is required from a regulatory standpoint. The methods described in this report can be used to support evaluation of risk for any digital upgrade.

Example 2-3. Regulatory Perspective vs. Risk-Informed Perspective.

Digital controllers are installed in both redundant trains of an essential service water (ESW) system, which is initiated based on signals generated with ESFAS (example given in TR-102348 Revision 1, see Reference [3]). Although ESW is considered an engineered safety feature in this example, it is not part of the actuation system (ESFAS) as defined in the plant licensing basis (SAR). Therefore, it is concluded that a D3 evaluation is not required from a regulatory perspective.

However, from a risk-informed perspective, ESW could be an important contributor to mitigation of a number of accident sequences, which may be risk significant based on the plant's PRA. Therefore, the utility decides to perform a D3 evaluation as part of the design effort, to verify that postulated digital failures do not significantly increase plant risk.

2.2.4 Advantages and Limitations of Risk-Informed Methods

With the increasing acceptance of PRA into the regulatory environment and the completion of plant-specific PRAs for all operating plants, risk-informed methods are available to complement the traditional deterministic methods.

Use of risk insights can help overcome some of the shortcomings of the BTP-19 (see Reference [1]) Deterministic Method that are described in Section 2.1.4. In particular, use of the PRA and its accident sequences, which are broader in scope than the set of events considered in the SAR, provides a more complete assessment of the impact of digital upgrades on plant risk:

- In addition to the design-basis events described in the SAR, the PRA also includes a number of beyond-design-basis events.
- The PRA considers mitigating systems and functions that go beyond what is credited in the design-basis analyses.

Risk-informed methods use acceptance criteria based on overall plant safety, with acceptance criteria based on the potential for core damage and exposure of the public to radiation releases. This allows evaluation of digital upgrades in the context of the other potential contributors to plant risk. PRA analysis is best-estimate in the sense that it attempts to characterize the actual plant response to initiating events, available mitigating functions and systems, and their failure modes.

Incorporating digital upgrades in the PRA models allows comprehensive treatment of the digital systems reliability and benefits (see Section 4.4.5) Also, for most plants, the PRA will need to be updated at some point to reflect digital upgrades, regardless of whether it is used to support D3 evaluations. Thus, updating the PRA to support D3 evaluations will put the plant further along in its efforts to keep its PRA up-to-date.

An additional benefit of risk-informed techniques is the capability to help optimize the design of a digital upgrade from both safety and plant performance standpoints. These techniques can be used to systematically evaluate prospective I&C architectures, including consideration of design complexity that could lead to reduced reliability and increased risk. Also, the designer can use the resulting risk insights to guide design decisions and focus efforts on the areas of greatest risk.

A potential limitation of the quantitative risk-informed methods is the need to establish failure effects and probability values for digital failure and digital CCF. Methods for identification of specific failure modes, modeling the effects of these failures, and assigning failure probabilities for these events are evolving. However, in many cases, it is possible to obtain the needed risk insights by modeling the functional effects of digital failures, rather than the internal details of the digital systems and their specific failure modes (see Section 3.1.2). To address uncertainty concerns, for the purpose of D3 evaluation, conservative or bounding values can be used for failure probabilities and beta-factors. Alternatively, a combination of best-estimate values and sensitivity studies can be used.

3
GUIDANCE ON PERFORMING D3 EVALUATIONS

This section provides general guidance on performing D3 evaluations. It gives an overview of the D3 evaluation process, and describes three methods that are recommended as alternatives to the BTP-19 (see Reference [1]) deterministic evaluation approach:

- An "Extended Deterministic" method based on BTP-19 but with risk insights applied.
- A "Standard Risk-Informed" method based on use of the PRA modified to reflect the digital upgrade.
- A "Simplified Risk-Informed" method that uses data from the existing, unmodified PRA.

All three methods are blends of deterministic and risk-informed approaches. Any one of the three methods is sufficient to meet the intent of BTP-19 and demonstrate that vulnerabilities to digital CCFs have been adequately addressed. However, more than one of these methods can be applied to provide additional assurance of adequate defense.

The process shown in Figure 3-1 assumes that the digital upgrade project has progressed to a point where sufficient design information is available to identify susceptibilities to digital failures and digital CCFs. However, plants are encouraged to evaluate D3 issues early in a project (e.g., at the conceptual design stage), examine design options and tradeoffs, and determine a final architecture that best manages the risk impact and other considerations related to the upgrade. The methods described in this section for the formal D3 evaluation can also be used to support such conceptual design studies.

As shown in the figure, the D3 evaluation process consists of five steps:

1. Determine whether a D3 evaluation should be performed for the current project. Both regulatory and risk perspectives should be considered (see Sections 2.1.3 and 2.2.3).
2. Determine what susceptibilities to digital failure and digital CCF need to be addressed in the D3 evaluation. Guidance for this step is given in Sections 3.1 and 4.2.
3. Choose the D3 evaluation method that will be used. Guidance on the trade-offs is provided in Section 3.7, which summarizes and compares the methods presented in this guideline.
4. Perform the evaluation using the chosen evaluation method. Sections 3.2, 3.3, and 3.4 describe the three methods presented in this guideline. Other methods may be appropriate with corresponding technical justification. In addition to method-specific acceptance criteria, the methods in this guideline all include a confirmatory review step that is discussed in Section 3.5. If the acceptance criteria are not met or the confirmatory review reveals potential problems, then the upgrade design is revised and/or the evaluation is refined and the D3 results reassessed (see Section 3.6). Section 4 provides more detailed guidance and information on use of the methods.
5. Document the results. Section 4.6 provides guidance on documentation.

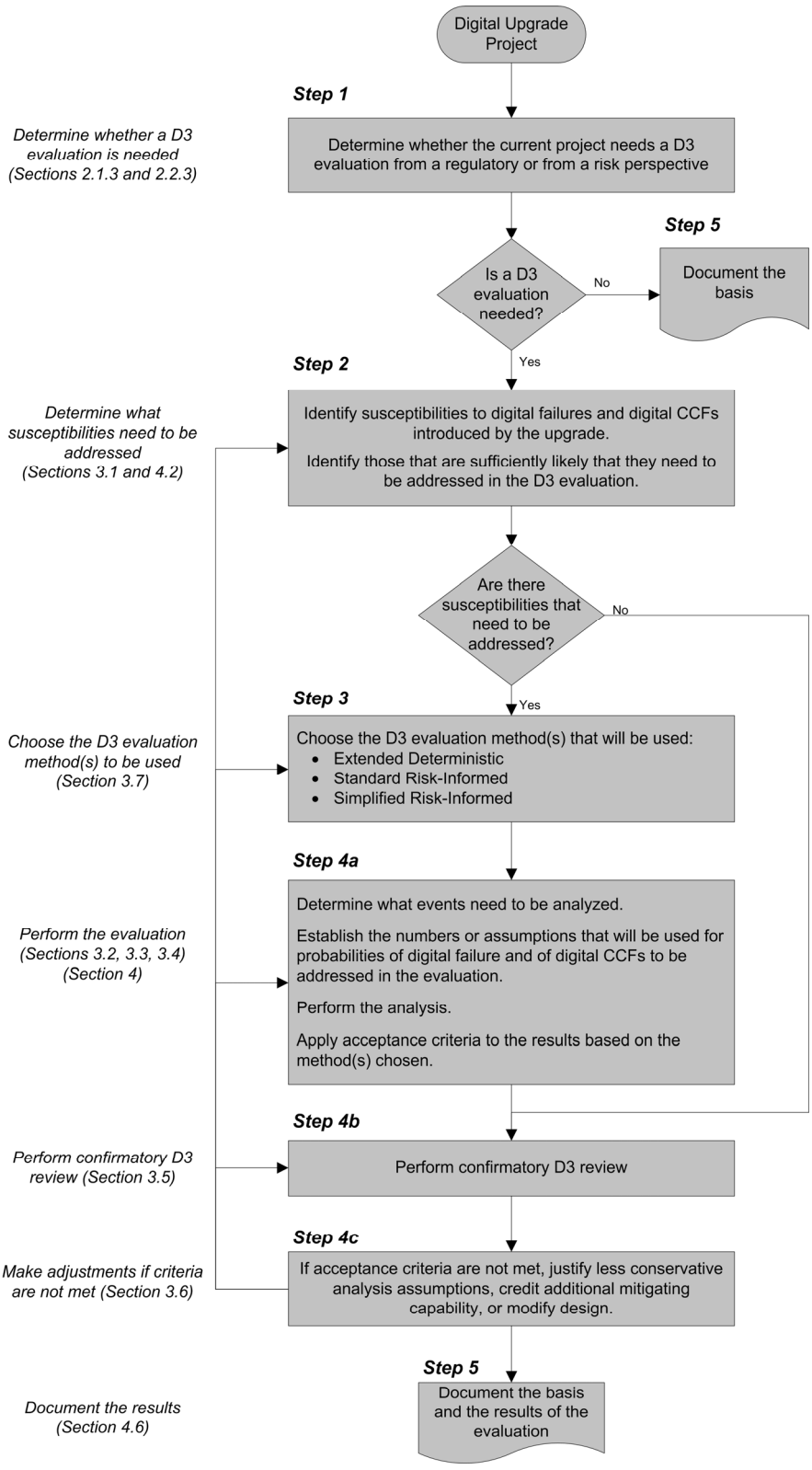

Figure 3-1
Overview of the D3 Evaluation Process Using Alternatives to the BTP 19 Deterministic Method

3.1 Identification of Susceptibilities to Digital Failures and Digital CCFs

The second step in the D3 evaluation is to identify the susceptibilities to digital failures and digital CCFs that should be addressed. This deterministic process defines the scope of the subsequent D3 evaluation. The following subsections describe and contrast the current regulatory guidance and the approach proposed in this guideline.

3.1.1 NUREG/CR-6303 Approach

NUREG/CR-6303 (see Reference [5]) provides guidance on identifying susceptibilities to digital CCFs. In particular, it states that:

- "*A block diagram of the system to be analyzed should first be constructed.*"
- A block is "*a physical subset of equipment for which it can be credibly assumed that internal failures, including the effects of software errors, will not propagate to other equipment or software.*"
- "*Candidate blocks should then be examined under the Diversity Guideline, to decide which blocks are identical for analysis purposes, and which will be considered diverse.*"

It also states that "*blocks are to be considered identical ... when the likelihood of a CMF affecting them simultaneously is not acceptably low.*"

3.1.2 Defensive Measures Approach

To identify susceptibilities to digital failures and digital CCFs, the "Defensive Measures" approach presented here essentially follows and extends the NUREG/CR-6303 approach. The main differences are that:

- It can be used not only in deterministic D3 evaluations, but also in risk-informed D3 evaluations.
- It allows the susceptibilities identification process to be tailored based on the relative importance of the three factors as determined by the D3 evaluation method selected. For example, the Simplified Risk-Informed Method relies primarily on factor A, assigning best-estimate digital failure probabilities, and uses conservative simplifying assumptions to address factors B and C. The Extended Deterministic Method considers primarily factors B and C, assessing susceptibility on a yes-or-no basis; however, for problematic events where risk insights are applied, it may use all three factors on a best-estimate basis.
- It can take into account defensive measures that include, but are not restricted to, the seven diversity attributes listed by NUREG/CR-6303.

Crediting Defensive Measures in D3 Evaluations

The basis of the Defensive Measures approach is to provide insights on the potential digital failure and digital CCF mechanisms, through the consideration of design features and functional characteristics that can restrict such mechanisms to a small manageable set of possibilities.

When used as part of the Extended Deterministic Method, this approach can help determine, based on deterministic arguments, the effectiveness of diversity attributes and other defensive measures against digital CCFs. In favorable cases, consistent and appropriate sets of measures may provide reasonable assurance that even blocks that share identical digital design elements have an acceptably low likelihood of digital CCF.

When used as part of the Standard or the Simplified Risk-Informed Method, the Defensive Measures approach can help determine where digital failures and digital CCFs need to be considered. When needed, it can help estimate reasonable probabilities of digital failures (P_{DF}) and concurrent digital failures (beta-factors) for use in PRA analysis.

Choosing Blocks

The Defensive Measures approach begins with the construction, as suggested by NUREG/CR-6303, of a system block diagram that shows the primary actuation paths associated with the system being upgraded. The level of detail in the diagram can depend on the desired degree of precision of the susceptibilities identification: simplified diagrams usually give more conservative results; detailed diagrams may have more accurate and realistic results. The desired degree of precision can depend on the D3 evaluation method being used, and on the impact on plant risk of the functions being evaluated.

For example, when using the Simplified Risk-Informed Method, the analyst can start with:

- Readily accepted (and very conservative) values for the probability of digital failure (P_{DF}) of the digital equipment, and
- The simplifying (and also very conservative) assumption that all digital failures are also digital CCFs (beta-factors of 1, see Section 3.4.2).

Then, each digital system or device can be represented by a single block, and the second step of the D3 evaluation process is complete.

However, if after having completed the D3 evaluation, it is concluded that the D3 acceptance criteria are not met, then one option is to perform a more realistic and less conservative susceptibilities identification (see Figure 3-1): this would usually require a more detailed system block diagram.

For higher degrees of precision, it may be worthwhile to decompose particular blocks to the limit defined by NUREG/CR-6303 (see Section 3.1.1). In some cases, it may also be worthwhile to go even further and to decompose particular elementary blocks into modules that would not qualify as blocks, per NUREG/CR-6303. Guidance concerning the selection of blocks and modules is provided in Section 4.2.6.

Identifying Susceptibilities

If the probabilities of digital failure of blocks, and the beta-factors between blocks do not have readily accepted values, the Defensive Measures approach suggests the following activities to justify or estimate these values:

- Identification of the system elements that are susceptible to digital faults. These typically include the functional specification, programmable equipment (e.g., programmable logic controllers (PLCs)), and "smart" devices.
- Determination of the types of digital faults that could affect each susceptible element, the operational conditions that could activate these faults, and the failure modes that could result. To this end, it may be useful to further decompose blocks into modules that could be examined individually for failure analysis purposes (see Section 4.2.6).
- Identification and characterization of the defensive measures in place to avoid or eliminate these faults, and to minimize the activating conditions that could concurrently trigger digital failures in redundant blocks.
- Assessment of the effectiveness and completeness of the defensive measures.

Different sets of defensive measures may be credited for different types of susceptible elements. Measures may concern the element itself, the way the element is used in the digital system, or the operational environment of the digital system. They may address aspects such as:

- Development, modification, and verification processes that provide reasonable assurance of fault avoidance and/or removal for the identified types of digital faults. EPRI-TR 102348 Revision 1 (see Reference [3]) provides guidance and further references on the development, modification, and verification processes of digital systems and software.
- Operational experience, giving reasonable assurance of reliability and appropriate behavior in similar conditions of use. EPRI-TR 106439 (see Reference [22]) provides guidance for the evaluation and acceptance of commercial grade digital equipment, based in particular on an evaluation and acceptance process.
- Logical separation and independence of redundant channels and systems, giving reasonable assurance that failures will not propagate beyond block limits. Additional guidance is provided in IEEE 603 (see Reference [21]).
- Functional characteristics of the plant system that may be used to minimize the likelihood of having unsafe digital failures (e.g., existence of an unequivocal and easy to reach safe failure position).
- Design features giving assurance that:
  - The level of residual faults is appropriately low (e.g., simplicity, modularity).
  - Unanticipated operational conditions that could cause a potentially unsafe digital failure are very unlikely (e.g., identification, minimization, and coverage of all factors that could influence the behavior of a block or module).
  - There is a good capacity for fault tolerance (e.g., surveillance, fail-safe orientation).

– Only limited parts of the design can be affected by operational conditions that could trigger potentially unsafe digital failures (modularity).

The last two bulleted items, functional characteristics and design features, are perhaps the most significant considerations in the identification and evaluation of susceptibilities. Functional characteristics of interest are determined primarily by behaviors at the plant system level. Design features refer to behaviors determined by the internal architecture and features embedded in the software and hardware of the digital equipment. Investigation of design features goes well beyond product marketing information and usually involves "white-box" analysis (i.e., analysis based on a detailed knowledge of the contents and design of the system). Sections 4.2.1 through 4.2.3 list typical defensive measures for the most common types of susceptibilities. Particular attention should be given to defensive measures against functional specification faults. Experience provides compelling and converging evidence that for high quality digital systems, these faults have often been the dominant cause of digital failure (see Reference [27]). For redundant channels implementing the same faulty functional specification, such failures are likely to be concurrent and result in CCFs, regardless of design, software or equipment diversity.

3.2 Extended Deterministic Method

This method is an extension of the BTP-19 (see Reference [1]) Deterministic Method, designed to address some of its shortcomings (see Section 2.1.4). Figure 3-2 provides an overview. The basic differences between the BTP-19 and the Extended methods are:

- The Extended Deterministic Method recommends crediting defensive measures (see Sections 3.1 and 4.2) to the extent that they limit susceptibilities to digital failures and digital CCFs. The BTP-19 Deterministic Method credits various types of diversity, but does not consider other valid types of defensive measures.
- The Extended Deterministic Method includes a confirmatory review to check for risk-significant events that might have been overlooked by the BTP-19 Deterministic Method (see Section 3.5).
- For initiating events where the relaxed acceptance criteria of the best-estimate deterministic analysis are not met, the Extended Deterministic Method provides the option of applying risk-informed insights and methods to assess the risk significance of the proposed plant modification for those events (see Section 3.6).

Otherwise, the Extended Deterministic Method is identical to the BTP-19 Deterministic Method, including use of the guidance of BTP-19 and NUREG/CR-6303 (see Reference [5]). In particular:

- NUREG/CR-6303 states "*Diversity and defense-in-depth analyses should be performed when credible potential exists for common-mode failure.*"
- BTP-19 requires that each initiating event analyzed in the SAR be evaluated concurrent with each postulated software common mode failure (replaced with digital CCF in this guideline).
- BTP-19 provides relaxed acceptance criteria for D3 evaluations compared to the acceptance criteria applicable to the SAR event analyses.

After determining that a D3 evaluation is needed (see Section 2.1.3) and confirming there are digital CCF susceptibilities that should be addressed (see Sections 3.1 and 4.2), the system block diagram is reviewed. For each of the initiating events analyzed in the SAR:

- The primary and backup mitigation functions for which credit is taken in the plant licensing basis are identified.
- A check is conducted to determine if any postulated digital CCF could degrade both the primary and backup mitigating functions.
- If such cases are found, then the initiating event is evaluated to determine if an additional mitigating function would be needed to meet the acceptance criteria.

These evaluations are done on a best-estimate basis as described in BTP-19, and the acceptance criteria are the relaxed acceptance criteria of BTP-19:

1. "*For each operational occurrence … analyses should not result in radiation release exceeding 10% of the 10 CFR 100 guideline value, or violation of the integrity of the primary coolant pressure boundary."*

2. "*For each postulated accident …analyses should not result in radiation release exceeding the 10 CFR 100 guideline values, violation of the integrity of the primary coolant pressure boundary, or violation of the integrity of the containment."*

Several approaches may be considered for demonstrating that adequate defense-in-depth exists in the plant systems. These include:

- Demonstration that no protective action is required, because the plant attains a new steady state that meets the relaxed acceptance criteria.
- Taking credit for other plant equipment that is not susceptible to the postulated digital CCFs.
- Assuming manual operator action within a defendable period of time (keeping in mind that this is a best-estimate analysis), using controls and monitoring instrumentation that are not affected by the postulated digital CCFs.
- Modifying the proposed design such that the susceptibility to digital CCFs is reduced.
- Adding an automatic mitigating or actuation function that is not affected by the postulated digital CCFs such that the plant response meets the applicable relaxed acceptance criteria.
- Using one of the two risk-informed methods of this guideline to evaluate specific events for which the BTP-19 acceptance criteria are not met when best-estimate analyses are used. Risk-informed analysis may demonstrate that risk is adequately managed for these events (see Sections 3.3 and 3.4).

The Extended Deterministic Method recommends a confirmatory D3 review (see Section 3.5) in addition to the SAR event analyses, and possibly risk-informed analyses of selected events, to help ensure that the deterministic focus on the SAR events has not resulted in missing safety-significant events. If either the BTP-19 relaxed acceptance criteria are not met, or the confirmatory review reveals events for which the available D3 might not be adequate, then the designer should consider options for refining the evaluation parameters and/or modifying the design (see Section 3.6). The final step is documenting the results of the evaluation (see Section 4.6).

The Extended Deterministic Method partially addresses two of the three important-to-risk factors of Section 2.2.2:

- Factor B, "potential for digital CCF" - The potential for digital CCF is considered on a block-by-block basis, and ultimately assumed to either not occur, or occur with certainty.
- Factor C, "plant design / safety model" - The method allows the designer to evaluate the adequacy of the design of the mitigating systems in response to each initiating event analyzed.

Factor A, "impact of the upgrade on I&C channel reliability" is not addressed, as the method does not consider the reliability of the mitigating functions. The designer assumes digital failure regardless of the expected or demonstrated reliability of the digital equipment.

3.3 Standard Risk-Informed Method

In the Standard Risk-Informed Method, the PRA model is updated to include key characteristics of the digital upgrade, and the PRA results are regenerated to estimate new core damage frequency (CDF) and large early release frequency (LERF) values. This method recognizes that the plant design already defines an implicit level of D3 that is predominately defined by the mechanical and electrical mitigating systems. The PRA includes a large portion of the mechanical and electrical mitigating equipment in the modeling and quantification of core cooling and containment systems. As a result, it is well-suited to assess whether a digital upgrade is capable of maintaining the existing D3 and to determine where digital failures will have only a limited impact on safety.

Figure 3-3 provides an overview of the method. First, a review of the PRA model is used to identify the elements that are potentially impacted by the upgrade. This begins with identification of initiating events and mitigating systems that may be affected. PRA elements of interest will include:

- Initiating events and frequencies (including what fraction might be caused by I&C failures).
- The specific trains into which the digital equipment is to be installed.
- New dependencies within and across systems that may be introduced by the digital upgrade.

Elements of the PRA model affected by the digital upgrade are updated (see Section 4.4) and the PRA results are regenerated. Sensitivity studies are used to assess the importance of uncertainties regarding digital failure probabilities and beta-factors. Acceptance criteria for the Standard Risk-Informed Method are based on the guidance of Regulatory Guide 1.174 (see Reference [2]), which defines acceptable changes in CDF and LERF. In addition to the probabilistic calculations, the Standard Risk-Informed Method recommends a confirmatory defense-in-depth review (see Section 3.5) to confirm the results of the quantitative analysis from a qualitative perspective. If either the Regulatory Guide 1.174 acceptance criteria are not met or the confirmatory review reveals events for which the available D3 might not be adequate, then options for refining evaluation parameters and/or modifying the design should be considered (see Section 3.6). The final step is documenting the results of the evaluation (see Section 4.6).

The Standard Risk-Informed Method addresses all three of the important-to-risk factors of Section 2.2.2:

- Factor A, "impact of the upgrade on I&C channel reliability" - The effects of postulated digital failures are explicitly represented using failure probabilities, in a manner similar to those of random failures of other components, but taking into consideration the deterministic nature of digital failures (i.e., activation of residual digital faults by unanticipated operational conditions; see discussion of factor A in Section 2.2.2).
- Factor B, "potential for digital CCF" - The identified intra and inter-system susceptibilities to digital CCFs are represented by beta-factors affecting redundant trains or systems.
- Factor C, "plant design / safety model" - The PRA model naturally integrates the effects of postulated digital failures and digital CCFs into the plant systems. Thus, the regeneration of the CDF and LERF calculations allows a direct assessment of the effect of the digital upgrade on the D3 that inherently exists in the design of the plant mitigating systems.

Section 4.4.5 discusses the incorporation into the PRA of the other positive and negative effects of the digital upgrade on the plant.

3.4 Simplified Risk-Informed Method

This section outlines a simplified, but bounding method to quickly assess the potential D3 implications of a proposed digital upgrade. It uses selected information from the plant PRA and can be applied without the need to update the PRA or perform the best-estimate accident analyses suggested by BTP-19 (see Reference [1]). As with the Standard Risk-Informed Method, the Simplified Risk-Informed Method recognizes that there is an implicit level of diversity and defense-in-depth that already exists in the plant design. The objective of the method is to assure that this level of D3 is maintained where it has value.

The basic principle of the method is to combine key information from the existing plant PRA with a conservative treatment of the effects of postulated digital failures to generate bounding estimates of the potential change in core damage frequency (ΔCDF) and large early release frequency (ΔLERF). If, under these bounding assumptions, ΔCDF and ΔLERF meet regulatory guidance (per Regulatory Guide 1.174, see Reference [2]) for a small change in risk, then the D3 evaluation is essentially complete, as it demonstrates adequate defense against digital CCFs. A confirmatory review still is performed per Section 3.5, as it is for the other two methods.

Figure 3-4 provides an overview of the method. First, a review of the PRA model is used to extract information needed to calculate the ΔCDF and ΔLERF estimates for each initiating event. The plant-specific PRA information needed is:

- The initiating events included in the PRA and their frequencies (including what fraction would be caused by I&C failures).
- A listing of front line mitigating systems available to respond to each of these initiating events.
- Time available for operator action to manually initiate mitigating systems for each initiating event (where manual initiation is to be credited in the D3 evaluation).

- Probability of failure (conditional on the initiating event) of mitigating systems that can be shown to be independent from the initiating event (performed only where the D3 evaluation finds that the cause of the initiating event is digital system-related and can also affect one or more of the mitigating systems).
- Conditional probability of large early release for each initiating event (for use in estimating ΔLERF from ΔCDF).

ΔCDF and ΔLERF estimates are then calculated for each initiating event (see Section 3.4.1). Acceptance criteria for the Simplified Risk-Informed Method are based on Regulatory Guide 1.174, which provides guidance on acceptable changes in CDF and LERF. In addition to the probabilistic calculations, the Simplified Risk-Informed Method recommends a confirmatory D3 review (see Section 3.5) to reaffirm the results of the quantitative analysis from a qualitative perspective. If either the Regulatory Guide 1.174 acceptance criteria are not met or the confirmatory review reveals events for which the available D3 might not be adequate, then the designer should consider refining evaluation parameters and/or modifying the design (see Section 3.6). The final step is documenting the results of the evaluation (see Section 4.6).

As with the Standard Risk-Informed Method, the Simplified Risk-Informed Method addresses all three of the important-to-risk factors of Section 2.2.2:

- Factor A, "impact of the upgrade on I&C channel reliability" - The effects of postulated digital failures are explicitly represented using failure probabilities, in a manner similar to those of random failures of other components, but taking into consideration the deterministic nature of digital failures (i.e., activation of residual digital faults by unanticipated operational conditions; see discussion of factor A in Section 2.2.2).
- Factor B, "potential for digital CCF" - The intra and inter-system susceptibilities to digital CCFs are represented by beta-factors between affected trains or systems.
- Factor C, "plant design / safety model" - The PRA model naturally integrates the effects of postulated digital failures and digital CCFs into the plant systems. Thus, the ΔCDF and ΔLERF calculations allow a direct assessment of the effect of the digital upgrade on the defense-in-depth and diversity that inherently exists in the design of the plant mitigating systems.

Note that as a first approximation, the method may use simplifying assumptions for factors B and C (see Section 3.4.2). The results of the Simplified Risk-Informed Method are considered conservative or bounding for several reasons:

- The method takes little credit for design features that likely make the reliability of the new equipment better than that of the equipment being replaced (including fault tolerance and self-diagnostics).
- The method assumes that all failures of the digital systems are potentially common cause, including random hardware failures.
- It further assumes that the redundant channels of a digital system will always fail simultaneously (intra-system beta-factor of 1). This is not always the case, even for identical channels, as a number of digital failures may be triggered by events that are unlikely to affect all channels simultaneously (see Figure 2-2 and Section 4.2).

- It also assumes that all failures of mitigating digital I&C prevent the affected plant systems from performing their safety functions (In some cases an I&C failure will not disable its system).

3.4.1 Using Parts of the PRA to Calculate a Change in Risk

For a given initiating event, the estimate for ΔCDF is based on the initiating event frequency from the PRA, the estimated probability of digital failure of a single channel of digital equipment, and the beta-factors representing digital CCFs. The beta-factors are considered within each mitigating system, between mitigating systems, and between mitigating systems and systems that can cause the initiating event.

The following simple relationships approximate the change in risk for each initiating event (assuming all beta-factors are 1):

ΔCDF =	Frequency of the initiating event (digital plus non-digital causes)	*	Probability of digital failure of the mitigating systems

ΔLERF =	ΔCDF	*	Conditional LERF for the affected initiating event

When there is a digital failure that can lead to a given initiating event, **and** when this digital failure also can affect one or more mitigating systems that are credited by the PRA, then the equation for ΔCDF will include two terms:

ΔCDF =	Frequency of the initiating event (digital plus non-digital causes)	*	Probability of digital failure of the mitigating systems
	+		
	Frequency of the digital failures that may cause the initiating event	*	Non-digital failure probability of the mitigating systems that are independent of the cause of the initiating event.

The new contributions to risk for each initiating event are summed to calculate a total ΔCDF and ΔLERF. The individual contributions from the initiating events are then examined to identify and investigate the dominant risk contributors.

3.4.2 Key Simplifying Assumptions

The Simplified Risk-Informed Method is applicable under the conditions that the digital upgrade does not significantly alter (i.e., increase) the frequencies of the PRA initiating events, and that a single channel of digital I&C of a mitigating system is at least as reliable as the equipment it replaces. These conditions should be confirmed through evaluation of the specific equipment design and quality attributes (see Sections 3.1 and 4.2). They are usually satisfied by upgrades that replace analog I&C systems with functionally equivalent digital systems. This might not be the case for digital designs that introduce significant new complexity or functional changes.

The following initial assumptions are made:

- All mitigating systems are subject to the effects of digital failures, including postulated digital CCFs (i.e., no credit is taken for the diversity of I&C platforms or defensive measures).
- Beta-factors of 1, regardless of whether mitigating systems share common elements.
- A digital failure that is postulated to cause an initiating event also results in loss of any mitigating system that has identical design elements.

These assumptions provide a bounding case, and may be refined with appropriate justification.

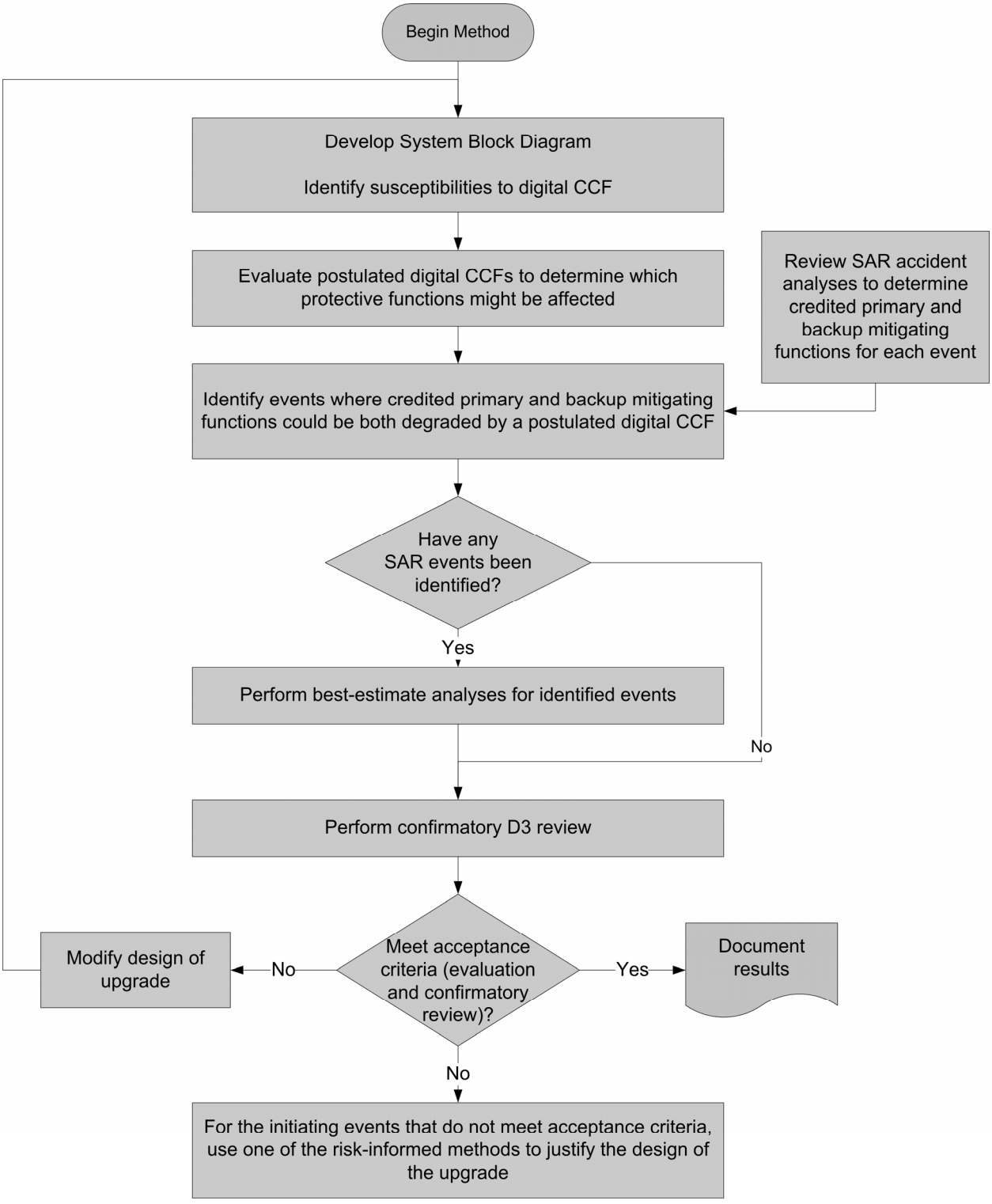

Figure 3-2
Extended Deterministic Method for D3 Evaluation

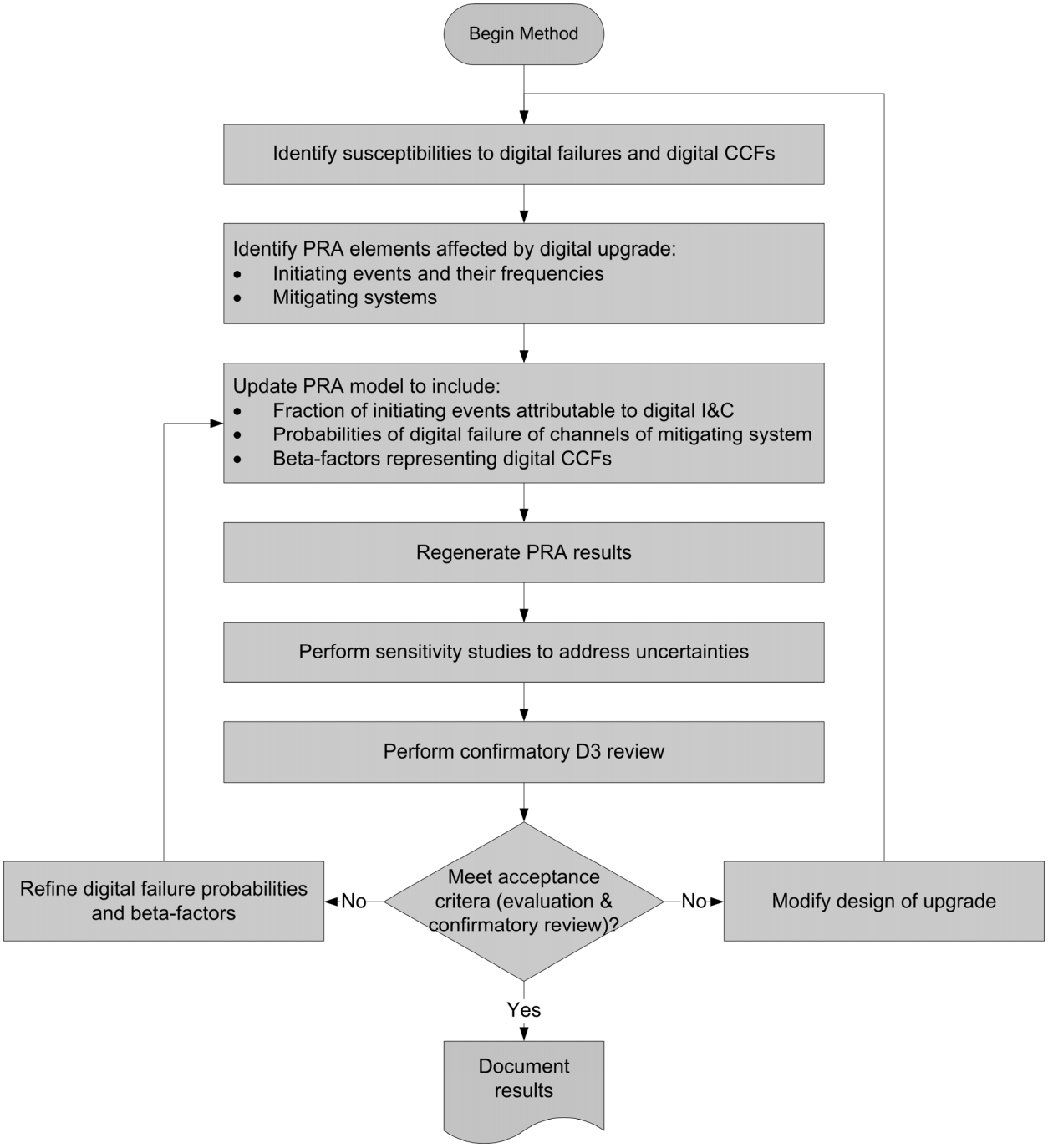

Figure 3-3
Standard Risk-Informed Method for D3 Evaluation

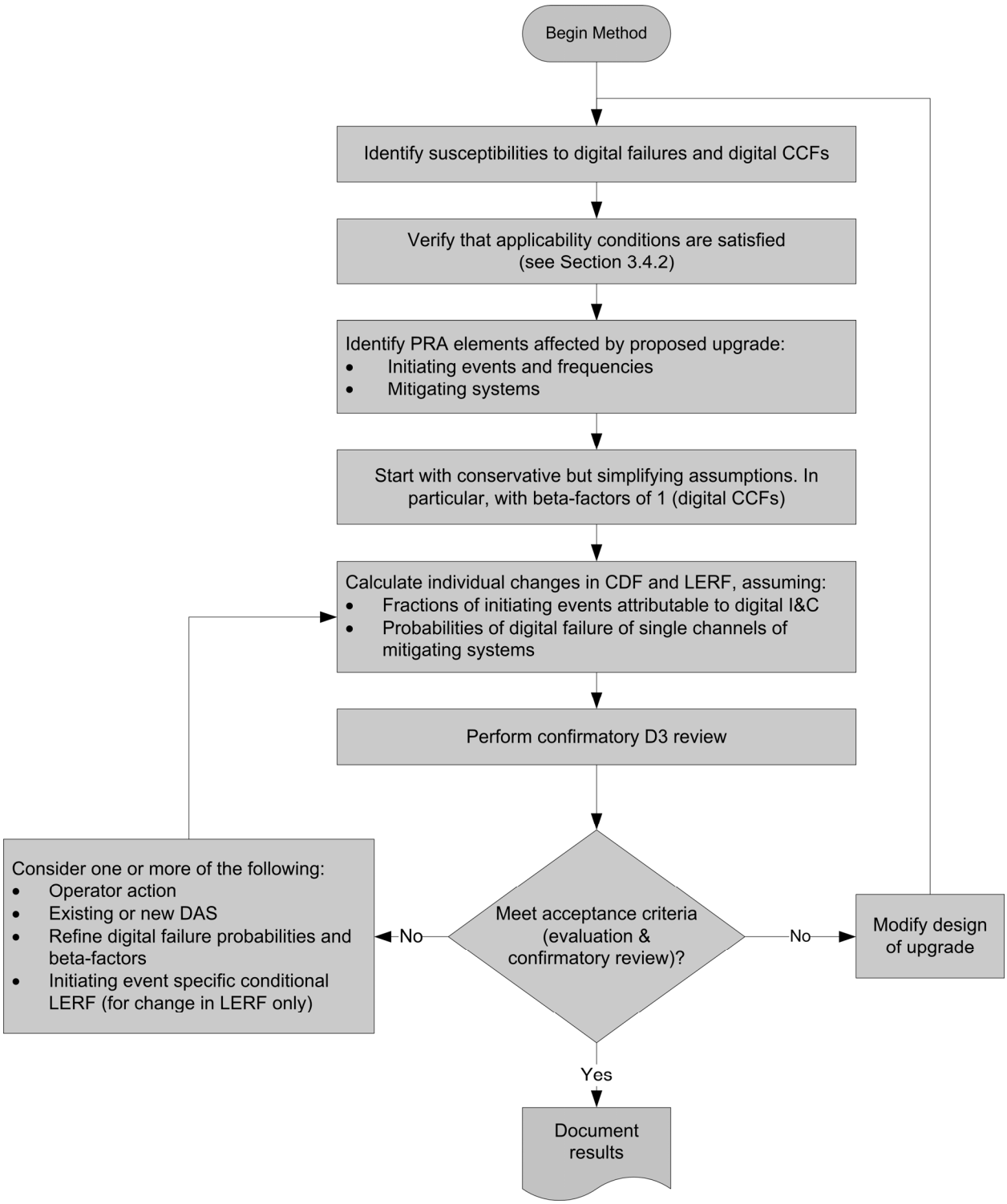

Figure 3-4
Simplified Risk-Informed Method for D3 Evaluation

3.5 Confirmatory D3 Review

Regardless of the D3 evaluation method used, it is recommended that a qualitative confirmatory review addressing both design-basis and beyond design bases events be performed. The objective is to confirm that the available systems provide adequate D3 for each of the initiating events. This approach is a blend of deterministic and risk-informed principles. It is risk-informed in the sense that the acceptable level of defense is a function of initiating event frequency, and deterministic in the sense that specific attributes of actual mitigating systems are considered.

For the Extended Deterministic Method, this step provides coverage of potentially risk-significant events that are not addressed under the BTP-19 (see Reference [1]) Deterministic Method. For the Standard and Simplified Risk-Informed Methods, this evaluation provides an understanding of the change in risk from a system design perspective, and documents compliance with the defense-in-depth principle of Regulatory Guide 1.174 (see Reference [2]).

Figure 3-5 shows an example of a blended deterministic/risk-informed approach that considers the full range of PRA initiating events. This approach is similar to that used routinely to assure adequate defense-in-depth when evaluating operating events in the Significance Determination Process (SDP) of the Reactor Oversight Program (see Reference[25]). The first column contains the PRA initiating events classified by their frequencies. The top row contains a spectrum of combinations of mechanical mitigating systems that offer decreasing levels of defense-in-depth going from left to right. The shaded area of the diagram represents acceptable levels of defense, as a function of the frequency of the initiating event (designated as the “green” or non-risk significant area in the SDP).

Added to the SDP diagram for the purpose of evaluating digital upgrades is a second row that contains examples of I&C system designs that cover a similar spectrum of defense-in-depth levels as the mitigating system configurations in the top row. In order to keep the example simple, each I&C system design spans two columns of the SDP diagram. For each I&C system design, the expected reliability is roughly equivalent to that of the leftmost corresponding mechanical system design in the top row. The shaded area of the diagram again represents acceptable levels of defense-in-depth, as a function of the frequency of the initiating event.

To use the Figure 3-5 approach, the designer compares the actual set of available I&C mitigating systems for each initiating event to the examples on the chart, and determines whether the corresponding D3 level is acceptable. For multiple mitigating systems to be credited, they should be shown to have an acceptably low likelihood of inter-system digital CCF (e.g., using the defensive measures approach as it is applied in the Extended Deterministic Method). In the same manner, they should also be shown to have an acceptably low likelihood of digital CCF with the causes of the initiating events. Design measures that protect against digital failures and digital CCFs (see Section 4.2) could be credited, as appropriate.

Example 3-1a. Using Figure 3-5 in Confirmatory D3 Reviews - Loss of Feedwater.

A plant-wide digital upgrade is being implemented. The digital CCF susceptibility evaluation has looked at the various digital platforms, applications and defensive measures and concluded that the safety and non-safety systems are effectively diverse; no digital CCFs between them need to be evaluated further (The possibility of digital CCF among safety systems, among non-safety systems, and among redundant channels also should be considered). A qualitative confirmatory D3 review is then performed for each of the initiating events in the PRA using Figure 3-5.

For the Loss of Feedwater initiating event, the primary mitigating system is Auxiliary Feed Water (AFW), a multiple train safety system that uses digital actuation and controls. There is also a backup digital actuation system for AFW, which is effectively independent, having no postulated digital CCF with the primary system I&C. Finally, there is hard-wired manual initiation capability for AFW, the Safety Injection (SI) pumps and Power Operated Relief Valves (PORVs) for feed-and-bleed purposes. The I&C design exceeds the capability described in the left most column of the second row of Figure 3-5, and therefore has adequate D3 for this initiating event.

Example 3-1b. Using Figure 3-5 in Confirmatory D3 Reviews - Large Break LOCA.

The Large Break LOCA (LBLOCA) initiator is mitigated by an automatic redundant digital safety system that actuates low head SI. Accident analysis indicates that the time available to initiate low head SI is not sufficient to credit manual operator action. Therefore, the I&C design for initiation of SI corresponds to that of the center column of Figure 3-5. Because of the low frequency of the LBLOCA, the availability of a single automatic, redundant safety system provides adequate D3 for this event, without additional means of actuating the SI function.

Figure 3-5 illustrates the Loss of Feedwater and Large Break LOCA confirmatory review examples.

Initiating Event Frequency	Mechanical System Designs	**≥ 3 diverse trains OR 2 redundant systems**	**1 train + 1 system with redundancy OR 2 diverse trains + recovery of failed train**	**2 diverse trains OR 1 system with redundancy + recovery of failed train**	**1 train + recovery of failed train OR 1 system with redundancy**	**1 train OR 1 system with redundancy (manual initiation with time constraints)**	**Recovery of failed train**	**None**
(Row added for the purpose of I&C confirmatory review)	**I&C System Designs** / **Initiating Events**	1 automatic redundant safety system AND (1 automatic I&C channel OR Manual initiation)		1 automatic redundant safety system OR (1 automatic I&C channel AND Manual initiation)		1 automatic I&C channel OR Manual initiation		
1 to 10 / yr	Reactor trip Loss of Condenser							
10^{-1} to 1 / yr	Loss of off-site power Total loss of main FW Stuck open SRV (BWR) MSLB (outside cntmt) Loss of 1 SR AC bus Loss of Instr/Cntrl air							
10^{-2} to 10^{-1} / yr	SGTR Stuck open PORV/SV MFLB MSLB inside Loss of 1 SR DC bus							
10^{-3} to 10^{-2} / yr	Small LOCA							
10^{-4} to 10^{-3} / yr	Medium & large LOCA							
10^{-5} to 10^{-4} / yr								
< 10^{-5} / yr								

Figure 3-5
Example of Approach for Confirmatory D3 Review

3.6 When Acceptance Criteria Are Not Met

The D3 acceptance criteria differ, depending on which evaluation method is used. The acceptance criteria for the Extended Deterministic Method are based on BTP-19 (see Reference [1]), whereas the criteria for the risk-informed methods are based on Regulatory Guide 1.174 (see Reference [2]). Acceptance criteria for the confirmatory review may be independent of method, as shown in the example of Section 3.5. If any of the acceptance criteria are not met, there are only a few basic alternatives:

1. Refine the parameters and/or assumptions used in the D3 evaluation (with justification).
2. Use one of the other D3 evaluation methods to gain additional insights to determine whether there is adequate D3.
3. Modify the design of the upgrade to eliminate the digital CCFs of concern.
4. Add a backup function that is not subject to the digital CCFs of concern.
5. Do not implement the upgrade.

Alternatives 1 and 2 above have different implications and limitations depending on which D3 evaluation method is being used. These variations are discussed in the following subsections.

3.6.1 Extended Deterministic Method

If the acceptance criteria of BTP-19 are not met, it may be possible to achieve acceptable results by crediting additional "best-estimate" considerations to remove remaining conservatisms from the SAR event analyses.

Alternatively, one of the risk-informed methods may be used to address the initiating events that proved problematic under the Extended Deterministic Method. Resulting risk-informed insights may be used to establish an engineering rationale as to why the design of the digital upgrade is acceptable, even though compliance with the BTP-19 relaxed acceptance criteria is in question. Such insights may include:

- The frequency of the event is sufficiently low that even conservative assumptions regarding the potential for digital CCFs would not result in the affected accident sequences contributing significantly to risk.
- Mitigating systems and/or operator actions not credited in the design-basis are available, which would prevent potentially significant consequences of the postulated digital CCFs.

If the acceptance criteria of the confirmatory D3 review are not met, it may be possible to credit additional existing features to show that the available mitigating systems offer better defense than was assumed in the failed evaluation. For example, there may be design features built into the software that limit the potential for digital CCF (see Sections 3.1.2 and 4.2), but were not credited in the original review in order to simplify the evaluation. Insights gained using risk-informed methods may also help determine the design changes that could lead to a successful confirmatory review.

3.6.2 Standard Risk-Informed Method

If the acceptance guidance of Regulatory Guide 1.174 is not met, it may be possible to achieve acceptable results by using less conservative, but still bounding probabilities of digital failures and beta-factors, if they can be justified. In addition, credit may be taken for defense-in-depth provided by existing means, such as operator actions or existing analog or other diverse actuation mechanisms that have not been previously considered. Another possibility might be to take more complete account of other positive impacts of the digital upgrade (e.g., initiating event frequency reduction due to improved monitoring of electrical/mechanical equipment).

3.6.3 Simplified Risk-Informed Method

The Simplified Risk-Informed Method has more limited options. Less conservative digital failure probabilities and beta-factors may be credited, with appropriate justification. However, if much adjustment is required, it may be more cost-effective to switch to the Standard Risk-Informed Method, so that all the impacts of the digital upgrade can be taken into account, e.g., reduction in initiating event frequencies due to improved reliability and diagnostics.

3.7 Summary and Comparison of Methods

Any one of the three alternative methods or a combination of them may be sufficient to demonstrate adequate D3. The designer therefore has flexibility to decide which is the most appropriate on a case-by-case basis. This section briefly discusses strengths and weaknesses of each method, presents a side-by-side comparison highlighting similarities and differences, and suggests a strategy for applying the methods in a sequence that optimizes the cost-effectiveness of the D3 evaluation.

3.7.1 Strengths and Weaknesses

All three of the methods are considered adequate in terms of addressing safety concerns. The strengths and weaknesses discussed here are based primarily on technical or logistical issues that could prove important, depending on the plant-specific or upgrade-specific circumstances. The following discussion briefly addresses each of the methods.

Extended Deterministic Method - This method is the closest to the BTP-19 (see Reference [1]), NUREG/CR-6303 (see Reference [5]) approach and is therefore the most familiar to both utility design engineers and regulators. It can use the same thermal-hydraulic codes used for the SAR analyses to perform the best-estimate analyses, with modified assumptions and initial conditions, and uses acceptance criteria based upon commonly used plant process parameters that are also used in the SAR analyses.

The primary weakness of the Extended Deterministic Method is that most of the initiating events are addressed using best-estimate analyses, which can be time consuming and expensive. Additionally, the best-estimate analyses will likely be unsuccessful for some events, which will then need to be addressed using risk-informed insights. Also, if the PRA model will have to be updated anyway, it may be more cost-effective to go directly to the Standard Risk-Informed Method.

Standard Risk-Informed Method - Although significant effort may be involved in modifying the PRA model, this may be a cost-effective alternative to performing best-estimate analyses under a deterministic approach. This method gives maximum flexibility in that it addresses all the affected failure probabilities and beta-factors independently. It also allows the analyst to credit other beneficial impacts of the upgrade, i.e., improved condition monitoring (see Section 4.4.5). It allows the risk impact of a particular digital upgrade design to be highlighted, explicitly identifying the accident sequence types and trains of equipment that drive risk. Performing PRA analysis early allows the upgrade design to be improved using risk insights and input from plant personnel knowledgeable in normal and emergency operations. Optimization of the design from a risk and cost perspective can be performed. Since the PRA model will need to be updated at some point to incorporate the upgrade, it may be advantageous to update the model early in the design process to support the upgrade effort (see Section 4.5).

A possible disadvantage of the method is that it could take longer due to scheduling and communications interactions between the design group and the PRA group, who would most likely perform the risk analysis. Depending on the extent of the upgrade, the level of detail with respect to the I&C currently included in the PRA, and the number of iterations with respect to the final design, update of the PRA potentially could take significant time to implement.

Simplified Risk-Informed Method - The principal advantage of this method is that it can be done very quickly compared to the other methods, and can be quickly revised as the upgrade design changes. Also, it can be implemented by non-PRA personnel with minimal assistance from PRA experts, as input from only a limited number of elements of the PRA is required. Like the Standard Risk-Informed Method, the Simplified Risk-Informed Method considers a broad spectrum of accident sequences that can be important to risk, including those that go well beyond the design-basis.

A potential disadvantage of the method is that it uses conservative or bounding assumptions in order to keep the methodology simple. Thus, it may result in the need to credit operator actions or provide additional backups that might be shown to be of limited importance if the Standard Risk-Informed Method were to be used, taking advantage of the full scope PRA.

3.7.2 Implementation Strategy

Table 3-1 summarizes the three methods in the context of the overall D3 evaluation process. It shows how the methods differ in terms of the events that are analyzed, the assumptions made regarding digital CCF likelihood, the analysis methods used, and the acceptance criteria applied to the results.

One suggested strategy for applying the methods is shown in Figure 3-6. With this approach, the Simplified Risk-Informed Method is applied first. This can be done relatively easily, and it provides insights into what events are most important from a risk standpoint. If this method gives acceptable results, it can be used by itself as the basis for demonstrating that the digital upgrade is acceptable from a D3 standpoint. (Of course, Extended Deterministic or Standard Risk-Informed analyses also could be performed to provide additional assurance, if desired.) If the Simplified Risk-Informed Method provides results that do not meet the Regulatory Guide 1.174 (see Reference [2]) acceptance criteria, then the sensitivity to the values used for probabilities of

digital failure and beta-factors may be reexamined. If there is a basis for using less conservative values in the events that dominate the results, the method should be repeated using the new values. If the method does not meet the acceptance criteria using values that can be justified, then either the Extended Deterministic or the Standard Risk-Informed Method is applied as the next step.

If the PRA can be expeditiously updated to support the D3 evaluation, then it is recommended that the Standard Risk-Informed Method be used. Again, there can be some iteration to identify the dominant contributors to risk and select appropriate failure probabilities and beta-factors.

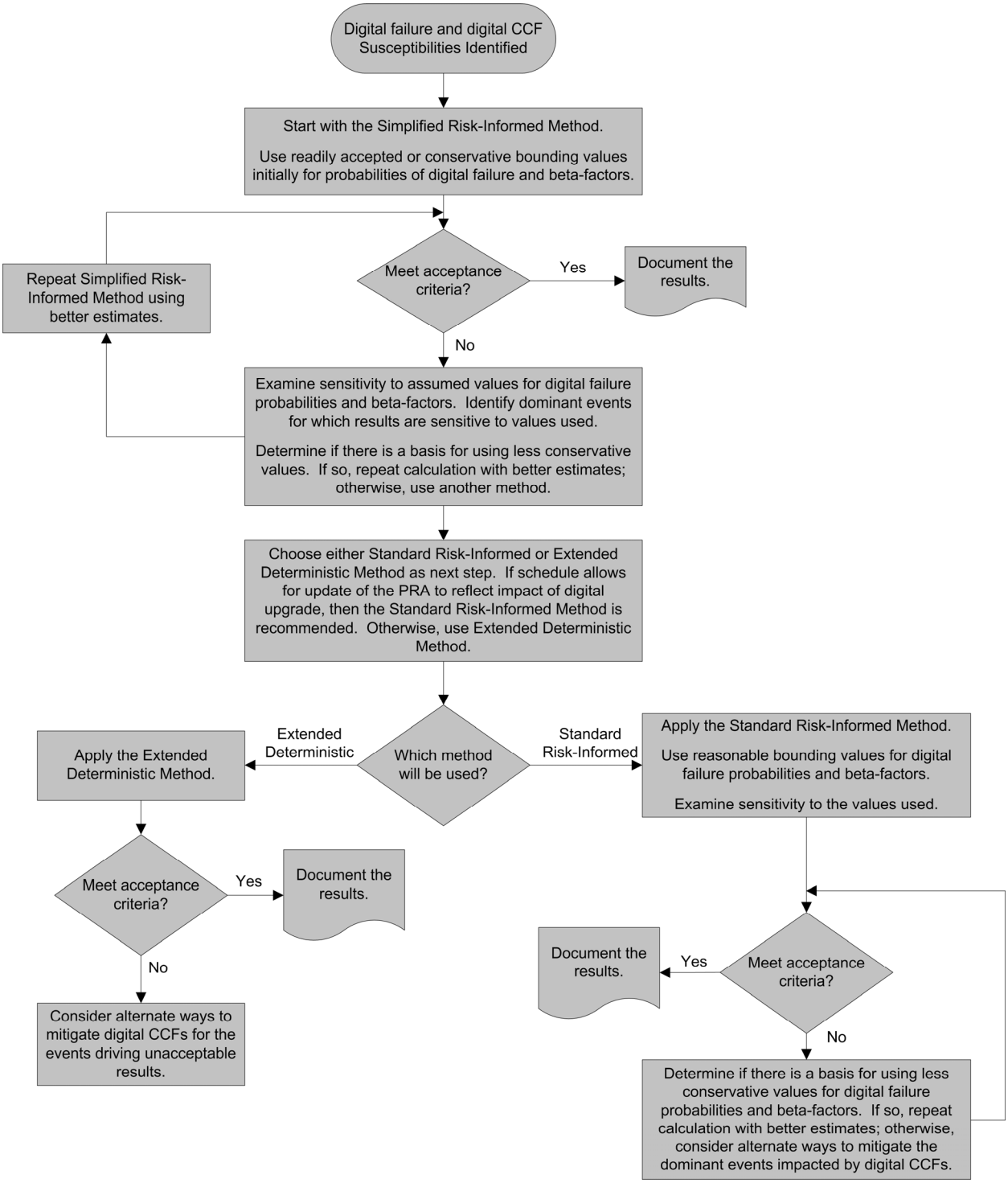

Figure 3-6
Suggested Strategy for Applying D3 Methods

Table 3-1
Summary of D3 Evaluation Methods

D3 Evaluation Steps	Extended Deterministic	Standard Risk-Informed	Simplified Risk-Informed
1 Determine if a D3 evaluation is required from a regulatory perspective	This is the case for: • Analog-to-Digital upgrades of RTS or ESFAS. • Digital-to-Digital upgrades to RTS or ESFAS that may affect previous D3 evaluation. • Upgrades affecting other systems credited in a previous D3 evaluation.		
2 Identify susceptibilities to digital CCF that need to be addressed	• Construct a block-diagram showing primary actuation paths affected by the upgrade. • Examine blocks to determine the likelihood of digital CCF (use Diversity Guideline of NUREG/CR-6303 or Defensive Measures approach of section 3.1.2, and consider failure propagation, including shared components and signals).		
3 Choose D3 evaluation method	Any one of the three methods can be used by itself. Suggested approach: start with the Simplified Risk-Informed Method; use the Extended Deterministic or Standard Risk-Informed Methods if necessary.		
4a Identify events to be analyzed	Initiating events analyzed in the SAR + those considered in the Confirmatory Review.	Initiating events included in the existing PRA	
4b Determine assumptions and values for PDF (probability of digital failure) and β (probability of conditional digital failure)	No quantified estimation of P_{DF}. β assumed to be 1 for blocks susceptible to digital CCF.	• Reasonable, bounding values for PDF and β. • Less conservative values if necessary and justified. • Sensitivity studies to examine effects of uncertainties.	• Initially: very conservative assumptions (bounding value for PDF, β=1). • Less conservative values if necessary and justified.
4c Perform analysis	"Best-estimate analysis" - using initial conditions and assumptions that are reasonably expected to occur.	• Update PRA to reflect effect of upgrade on initiating events and mitigating systems. • Recalculate CDF, LERF. • Calculate ΔCDF, ΔLERF.	• Use selected information from the existing PRA. • Simplified calculation of ΔCDF, ΔLERF for each initiating event.
4d Perform qualitative confirmatory review	Determine whether the available systems provide adequate D3 for each of the PRA initiating events (using for example a blended deterministic/risk-informed approach similar to the SDP of the Reactor Oversight Program).		
4e Apply acceptance criteria	Evaluation: relaxed criteria based on 10 CFR 100 and BTP-19	Evaluation: criteria defined in Regulatory Guide 1.174 for ΔCDF, ΔLERF.	
	Confirmatory Review: for example, criteria based on staying in the "green" area of the SDP defense-in-depth matrix.		
5 Document the D3 evaluation	**No D3 needed** (per step 1 above): briefly state the basis (may be as part of the normal upgrade process. **D3 as design aid**: documentation recommended but not required for licensing purposes **Scope of evaluation**: document the scope of changes to which the evaluation applies **Digital CCF susceptibilities**: document evidence showing that digital failure types are correctly identified, that credited measures provide adequate defense and were correctly implemented. (See also Section 4.6.1.) **Confirmatory D3 review**: see Section 4.6.4.		
	Analysis: see Section 4.6.2.	**Analysis**: see Section 4.6.3.	

4
ADDITIONAL GUIDANCE ON D3 EVALUATIONS

4.1 Susceptibilities to Random Hardware Failures

For digital equipment, both random hardware failures and software-based failures (called here digital failures) should be considered. High quality, redundancy, and separation are usually the main means to reduce the potential for system failure due to random hardware faults. Techniques for evaluating hardware failure probabilities are well established and are not discussed here in detail. From a hardware failure probability perspective, digital equipment does not require new evaluation methods, but it may offer significant advantages over the analog equipment it replaces. For example, digital equipment typically has fewer and more reliable hardware components. Various forms of fault tolerance can also be used in digital equipment, e.g., self-surveillance, surveillance by external means, or internal hardware redundancy and separation. Appropriate designs can reduce random hardware failures of digital systems to negligible levels.

4.2 Susceptibilities to Digital Failures and Digital CCFs

Regarding digital failures and digital CCFs, the primary defense is based upon high quality and dependability of the equipment and of the plant-specific application. As stated in BTP-19 (see Reference [1]), *"To defend against potential common-mode failures, the Staff considers high quality, defense-in-depth, and diversity to be key elements in digital system design. High-quality software and hardware reduces failure probability."*

Use of appropriate industry standards and regulatory guidelines for development, verification and validation, and configuration control helps ensure adequate quality and dependability of digital equipment for safety applications. However, quality and dependability are also profoundly influenced by factors other than engineering processes. For example, certain designed-in features and functional characteristics can help avoid or tolerate faults and cope with unanticipated conditions. Such measures are referred to as defensive measures. They may address either the engineering processes or the digital system design. The approach taken in this guideline is to credit all the defensive measures that help provide reasonable assurance that digital failures are unlikely, and digital CCFs are much less likely than single failures assumed as part of the plant's design and licensing basis.

This section gives examples of sets of defensive measures that could be considered when evaluating susceptibilities that might affect particular types of system elements. Section 4.2.1 gives examples of defensive measures addressing susceptibilities that might be caused by faults in the I&C system functional specification. Section 4.2.2 gives examples of defensive measures that address susceptibilities that might be caused by design faults in programmable equipment (e.g., PLCs). Section 4.2.3 gives examples of defensive measures that address susceptibilities that might result from design faults in smart devices with simple fixed functionality, such as smart transmitters.

Section 4.2.4 provides guidance for estimating probabilities of digital failure in individual I&C channels or devices. Section 4.2.5 provides guidance for estimating beta-factors associated with digital CCFs. Section 4.2.6 provides guidance for decomposing blocks into modules for the purpose of digital CCF susceptibility analysis and failure mode analysis.

4.2.1 Defensive Measures for Functional Specifications

Two main types of mistakes may lead to faults in the functional specification for the application of a digital system:

- Functional mistakes arise when incorrect understanding of the desired behavior of the digital system or of the behaviors of other plant systems or components is reflected in the functional specification. Such mistakes are usually not specific to digital systems, and have been found in the functional specifications of analog systems.
- Technical mistakes arise when the desired behaviors and functionality of the digital system are inaccurately or incompletely translated into the functional specification. Such mistakes result from various causes, including use of inappropriate functional specification methods and tools, or from insufficient or incorrect understanding of these methods and tools.

Table 4-1 lists a set of defensive measures and their potential benefits. Defensive measures for functional specification faults are primarily process related, particularly those that protect against functional mistakes. Although they are process focused, they often generate documentation that can be used to confirm their use after the fact.

Table 4-1
Examples of Defensive Measures for Functional Specifications

Defensive Measures	Benefits
Functional specification focused on what is strictly necessary for safety, and for the operation of the digital system.	Avoid functional mistakes, including: • Oversight of some of the operational conditions that may face the digital system. • Incorrect characterization of anticipated operational conditions. • Incorrect characterization of interfaces and interactions. • Specification of inappropriate behavior for some operational conditions. • Failure to specify actions and operational concerns for faults and failures • Failure to extend an existing system's logic into all operating conditions
Static and rigorous determination of all the entities interacting with the digital system, and of their different states.	
Functional specification addressing all resulting operational conditions.	
Simplicity of interfaces and interactions.	
Identification and examination of the differences with the I&C system to be replaced or with similar I&C systems that have proven to be adequate.	
Functional specification languages, elementary functions and tools with clearly defined and simple syntax and semantics.	Avoid technical mistakes, e.g.,: • Incompleteness. • Ambiguousness. • Insufficient accuracy. • Oversight of possible effects of digitization. • Oversight of possible adverse side-effects. • Intrinsically unsound expressions. • Incorrect translation of results of functional studies into functional specification.
Specification methods and tools well-adapted to application domain, allowing simple functional specification.	
Specification methods and tools that can help avoid or detect incompleteness and intrinsically unsound expressions (e.g., expressions that could lead to divisions by zero).	
Functional specification process guaranteeing that relevant functional studies are taken into account correctly.	
Functional specification process providing clear guidance regarding effects of digitization.	
Systematic verification of correctness and completeness of functional specification versus plant functional and safety requirements.	Reveals and removes existing functional specification faults.
Existence of an unequivocal and easy to reach safe failure position.	Reduce the likelihood of potentially unsafe failures.
Boolean safety outputs with clearly identified failure modes and unsafe failure modes.	
Plant operating conditions ensuring that potentially unsafe failures can occur only in particular situations (e.g., only during plant transients).	
Verification of functional specification particularly focused on potentially unsafe outputs.	
Specification of the conditions that should be satisfied by inputs (pre-conditions), and of conditions that must be satisfied by outputs (post-conditions).	

4.2.2 Defensive Measures for Programmable Equipment

With an appropriate set of defensive measures, digital design faults are very unlikely to be a dominant cause of digital failures and digital CCFs, even when different blocks contain identical software modules. Table 4-2 provides an example of a set of defensive measures that would be appropriate for programmable equipment. It relies heavily on "designed-in" features that are particularly effective against failures triggered by unanticipated operating conditions. These features are often recommended for high quality programmable equipment.

Table 4-2
Examples of Defensive Design Features for Programmable Equipment.

Defensive Measures	Benefits
Rigorous development and modification processes.	Low level of residual digital design faults.
Focus on safety, avoidance of non required components and capabilities.	
No generic susceptibilities (e.g., no management of time and date).	
Static allocation of resources.	
Deterministic behavior.	Rigorous identification and characterization of factors that can influence the functioning of software.
Invariability of software during operation.	
Validation of inputs prior to further processing.	
Clearly identified short term memory.	
Interrupts only for exceptions and clock.	
Cyclic functioning.	Among all these factors, only infrequent events are susceptible to cause digital failures.
Single-tasking.	
Limited amount of short term memory.	
Non- software watchdogs (failure of the digital system or channel to periodically reset a watchdog results in a specified safe action within a specified time frame).	Software deviations and failures are detected and lead rapidly to a safe position.
Surveillance of short and long term memory. Defensive programming.	
Rigorous operational procedures for operator requests (one channel at a time, only when absolutely necessary).	Service requests prevented from causing digital CCFs.
"Dissociation" of Operating System from Application Software.	Operating System prevented by design from causing potentially unsafe digital CCFs triggered by plant transients.
Transparency of Operating System to plant transients.	
Further decomposition of Operating System into dissociated modules.	Reduction of the likelihood of design faults in the Operating System.
Application Function Library composed of dissociated, simple, stateless, well-proven modules.	Application Function Library very unlikely to contain design faults that could lead to digital failures.

4.2.3 Defensive Measures for Smart Devices With Simple, Fixed Functionality

Table 4-3 lists a set of defensive measures that are particularly appropriate for simple devices. This set is based on a list of desirable attributes for the assessment of built-in quality of commercial grade smart devices introduced in EPRI TR 106439 (see Reference [22]). It includes process-related measures, designed-in features, and measures that can be applied by the user of the device to limit susceptibilities. While the defensive measures listed in Table 4-2 are generally for more complex devices, they may also be useful in simple devices.

Table 4-3
Examples of Defensive Measures for Smart Devices with Simple Fixed Functionality

Defensive Measures	Benefits
Application of documented and rigorous configuration management program.	Precise identification of the item, assuring that items with the same identification are identical.
Track record for control of changes and versions, and notification of changes (especially software fixes).	
Complete and unambiguous documentation.	Characterization of the item, stating in particular what it does, how well it does it, what is guaranteed it will not do, how it can fail, how it should be used, what it needs for correct operation.
Accurate documentation consistent with actual design.	
Adequacy to support needed functionality.	Fitness to purpose.
Unneeded / unused capabilities shown to have no adverse impact on required functionality.	
Rigorous development, manufacturing, and modification processes.	Low level of residual digital design faults.
Functional and technical simplicity.	
Sufficient amount of credible, relevant, and successful operating history.	
Testing in expected operational conditions.	
Error handling capabilities, built-in protective features, ability to handle expected and unforeseen errors and abnormal conditions and events.	Robustness, fault-tolerance.
Technical assurance that the device is used in narrow operational conditions, consistent with the bounds of its qualification.	Safe use of the device.
External surveillance by other portions of the I&C system, which increases the likelihood that failures or drifts are rapidly detected.	

4.2.4 Estimating Probabilities of Digital Failure (P_{DF}) of Individual I&C Channels or Devices

Realistic values of probabilities of digital failure (P_{DF}) are necessary for the purpose of PRA modeling. There is no generally accepted method for providing accurate figures. However, various factors may be considered when estimating failure probability.

Use of appropriate software development standards is one factor. IEC 61226 (see Reference [17]) states that "*For an individual system which incorporates software developed* in *accordance with the highest quality criteria (IEC 60880 and IEC 60987), a figure of the order of 10^{-4} failure / demand may be an appropriate limit to place on the reliability that may be claimed* (Note: IEC 60880 addresses software, while IEC 60987 addresses hardware.) Indeed, a number of regulatory agencies have accepted the use of a failure probability of 10^{-4} for digital equipment qualified for use in safety applications. This should be applicable in estimating the probability of digital failure of channels that use pre-qualified platforms with applications and configurations developed following current industry and regulatory guidance, and benefiting from measures such as those listed in Table 4-1.

Example 4-1a. Probability of Digital Failure Based on Software Development Standards and Defensive Measures for Applications and Configurations.

A PLC platform is being used as part of an ESFAS upgrade. The evaluation of the platform reveals that the supplier's software development and configuration management processes are based on the IEC 60880 standard. The review further confirms that the process steps were appropriately implemented and the corresponding documentation is in place in accordance with the standard. The application software and configuration for the PLC are developed by the utility under its 10 CFR 50 Appendix B QA program in accordance with applicable industry and regulatory guidance, and includes suitable defensive measures. In particular, the operating conditions that can affect the upgrade are systematically identified and are correctly characterized and addressed; all inputs are validated prior to any further processing. It is concluded, for the purposes of a risk-informed D3 evaluation and for updating the plant PRA, that an appropriate digital failure probability estimate for a single I&C channel based on the platform is 10^{-4} per demand.

Example 4-1b. Probability of Digital Failure Based on Use of "Pre-Qualified" Platform and Defensive Measures for Applications and Configurations.

An alternative to the PLC platform of Example 4-1a is being considered. The investigation of the platform reveals that the NRC has evaluated and "pre-qualified" it for safety applications in a safety evaluation report (SER). A review of the SER confirms that the NRC's acceptance criteria are at least as stringent as those of the IEC 60880 standard. It is concluded that if the application/configuration is developed by the utility as in Example 4-1a (i.e., under its 10 CFR 50 Appendix B QA program and with adequate defensive measures), an appropriate digital failure probability estimate for a single I&C channel based on the platform will again be 10^{-4} per demand.

Defensive measures such as those listed in Tables 4-2 and 4-3 constitute an important factor that helps ensure high dependability in digital systems, because by design, they preclude or mitigate various types of potential failure modes and digital CCFs. In principle, such measures can be used to achieve digital system reliabilities better than those of functionally similar analog channels of I&C.

Example 4-1c. Impact of Defensive Measures in a PLC Platform.

As part of the evaluation of the PLC platform of example 4-1b, a detailed "white-box" design review is conducted to better understand the potential failure modes, abnormal behaviors, and defensive measures designed into the platform (see Example 4-6b). This review provides additional assurance of high quality by looking beyond the primarily process-based assessment documented in the SER. Key behaviors and defensive measures are confirmed by review of documentation and/or testing. As in Examples 4-1a and 4-1b, the application is developed under an Appendix B program and has appropriate defensive measures. The evaluation concludes that the combination of the confirmed defensive measures in the platform and the application precludes nearly all the potentially unsafe digital failure types that are postulated for the intended plant application. For the purposes of the D3 evaluation and PRA update, the digital failure probability of a single I&C channel is assigned a value of 10^{-5} per demand.

Statistical evidence on the operational experience of comparable digital systems is another factor that may provide indication of bounding or practical estimates of digital failure probabilities for use in risk-informed evaluations. For example, digital flight control systems used in modern commercial aircraft have accumulated operational experience exceeding 10^4 years without a single report of a potentially unsafe digital failure. Digital equipment used in nuclear safety applications are also subject to extremely rigorous development and verification & validation processes, and under certain conditions (e.g., appropriate on-line monitoring assuring that they are fully operational), they could be credited with a comparable level of reliability.

Some of the PLC platforms and smart devices already in use in process industries (e.g., in chemical plants or oil refineries) may also be considered for use in nuclear power plants. When supporting critical applications, such equipment is usually under strict surveillance: vendors are required to apply rigorous version and configuration management, and any failure is likely to be detected, reported and analyzed (in particular assigning the cause either to random or digital origin). These failure reports and the corresponding cumulated volume of experience can provide an estimation of the probability of digital failure for conditions of use similar to those of the credited experience. Justification usually needs to be provided when the experience encompasses several versions of the product.

Example 4-2a. Probability of Digital Failure Based on Operational Experience.

A smart trip unit for circuit breakers is to be installed in the plant and incorporated into the plant PRA model. The evaluation of the operating history reveals that:

- The vendor has had, since product rollout, a comprehensive tracking process and organization to collect and address customer reported failures.
- Considering the functionality of the device and the customer and application profiles, failures (spurious actuations and failures to actuate) are very unlikely to go unnoticed and unreported.
- All the recorded failures have been random hardware failures; there have been no reported digital failures.
- The software and the digital design have not been modified since product rollout.
- Approximately 200,000 units have been deployed for several years, with an accumulated volume of operating history exceeding 10^6 years with no reported spurious actuation due to digital causes.
- Based on the application profiles, there are between 1 and 5 demands per unit per year, resulting in several million demands with no reported failure to trip due to digital causes.

Because of the limited functionality of the device, all the industry experience is considered relevant in assessing the device for the nuclear plant application. Based on the million plus successful operating years and the several million successful trip actuations, it is estimated that the probability of a digital failure is negligible compared to the probability of random hardware failure (which is also estimated based on the vendor records).

In Example 4-2a, the likelihood of digital failure was judged to be negligible compared to the likelihood of random hardware failure. If it can further be justified that the likelihood of digital CCF is sufficiently low that the beta-factor can be assigned a value of 0 (see Example 4-5), then the component will have negligible impact on plant risk, and there is no need to assign a value to the probability of digital failure.

Justification of a low probability of digital failure value will typically rely on detailed knowledge of such items as the supplier's software development process, the internal hardware and software architecture of the device, and the operating history and problem reports. This information goes well beyond what would normally be found in brochures, specification sheets and operating manuals. It may or may not be available for assessment, and obtaining it probably will require the cooperation of the equipment supplier.

Example 4-2b. Probability of Digital Failure with Limited Information.

An alternative device to the trip unit of Example 4-2a is investigated because of its advanced functionality. The evaluation reveals that:

- In tests performed in the utility's I&C lab, the device performs flawlessly.
- The development process and documentation are based on rigorous standards and are consistent with expectations for safety-related applications.
- This new addition to the product line has only been on the market for six months; about 2000 have been sold, but the vendor is reluctant to share the limited operating history data.
- While the device is based on earlier generations, it contains new proprietary algorithms that the supplier will not reveal because they are important to his competitive advantage in the marketplace.

Because of the supplier's reluctance to discuss the new algorithms, a detailed investigation of designed-in defensive measures is not possible. Also, because the device is new, it is not possible to credit the operating history. Without knowledge of the device internals, the completeness of the utility testing is open to question and is not heavily credited. Ultimately, the evaluation credits the strong development process and the relative simplicity of the device, and assigns a digital failure probability of 10^{-3} and a beta-factor of 10^{-1}. However, the PRA shows that using this failure probability and beta-factor, the trip unit may become a significant contributor to risk for some events. Thus, the utility opts to go back to the device of Examples 4-2a and 4-5.

4.2.5 Estimating Beta-Factors

General experience with rigorously designed and highly reliable digital systems shows that the predominant causes of digital failures are usually functional specification faults (see Reference [27]). A change in plant conditions that activates a functional specification fault and causes a digital failure is often likely to cause also a digital CCF of all the channels implementing that functional specification. The reason is that these channels (usually, they are internal redundancies of an I&C system) are likely to perceive the condition concurrently and identically (or nearly identically). Thus, intra-system beta-factors are often assigned a value of 1, even when the channels benefit from design, equipment or software diversity.

Example 4-3. Different Platforms Implementing the Same Functional Specification for the Same Mitigation Function.

The two PLCs from Examples 4-1a and 4-1b are to be used in redundant channels of the same ESFAS system. They come from different manufacturers and have diverse software and hardware. However, they are to be used to implement the same functional specification, for the same mitigating function. Considering the high quality of the PLC platforms, the effectiveness of the defensive measures taken against technical mistakes in the functional specification, and the rigor of the application software development process, it is estimated that, in this particular case, the most likely cause of digital failure is functional mistakes (see Section 4.2.1). Consequently, the intra-system beta-factor representing the digital CCF of the two channels is conservatively assigned a value of 1. Thus, there is no advantage to using diverse manufacturers, equipment and software in this case, and the system designer instead opts to use like platforms in the redundant channels.

The more interesting case is that of like platforms implementing different functions. With appropriate defensive measures, most types of functional specification faults are either very unlikely or unlikely to be causally related in diverse functional specifications in a manner that would cause digital CCFs. A possible exception could be the oversight of operational conditions resulting from the same misconception of the operational environment of the digital systems. An example of this might be a misunderstanding of how some other plant system would interact with the functions of interest during an initiating event. When this issue is correctly addressed (e.g., by measures such as those listed in Table 4-1), there is a reasonable assurance that the likelihood of inter-system digital CCF is at least an order of magnitude less than the probability of digital failure.

Example 4-4a. Like Platforms in Systems Implementing Similar Functions Activated in Different Plant Conditions.

The PLC platform from Example 4-1c is to be used in two different systems. One system implements automatic reactor trip on low pressurizer pressure. The other implements automatic auxiliary feedwater actuation on low steam generator water level. The algorithms and (analog) sensors are very similar. Also:

- Functional specifications and application software were developed under a 10 CFR 50 Appendix B QA program.
- Appropriate defensive measures have been taken against technical mistakes (see Section 4.2.1 and Table 4-1).
- Because of the protection coverage of the defensive measures, it is estimated that the most likely cause of digital failure is functional mistakes.

Because the plant dynamics associated with pressurizer pressure and steam generator level are not closely related during a Small Break LOCA, the inter-system digital CCF is not considered likely, and the beta-factor is conservatively assigned a value of 10^{-1}.

Example 4-4b. Like Platforms in Systems Implementing Very Different Functions.

The PLC platform of Example 4-1c is used in two different systems. One system controls a series of timed relay actuations, monitoring electrical power measurements to confirm proper operation. The other adjusts a throttle valve to control flow, using a flow measurement signal for feedback. The evaluation shows that:

- Functional specifications and application software were developed under a 10 CFR 50 Appendix B QA program.
- Appropriate defensive measures have been taken against technical AND functional mistakes that could cause digital CCFs (see Section 4.2.1 and Table 4-1).

Because of this and because the systems have very different functionality and monitor diverse, unrelated process parameters, the inter-system digital CCF is considered very unlikely. The analyst concludes that if the Extended Deterministic Method is used, the systems would **not** be considered susceptible to digital CCF. If one of the Risk-Informed methods is used, a conservative value for the beta-factor would be 10^{-2}.

For devices with simple and fixed functionality, and offering extensive defensive measures (such as those listed in Tables 4-2 and 4-3), the likelihood of digital failures and digital CCFs may be considered negligible.

Example 4-5. Beta-Factor for Simple Device.

The engineering evaluation of the trip unit of Example 4-2a determines that:

- It has been developed in accordance with a well-defined life cycle process that complies with industry standards and regulatory guidance.
- It is a very simple, easily tested device offering a fixed functionality.
- Substantial operating history has demonstrated high reliability in applications similar to the intended application.
- The software 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, no memory, no date and time.
- A separate alarm relay is available to annunciate detected failures.
- Failures are bounded by existing failures of the analog device.

Because this is a simple device backed by a strong development process, a design that uses appropriate defensive measures, and an operating history that is both extensive and successful, it is concluded that the likelihood of concurrent failures in multiple channels is acceptably low (e.g., less than the likelihood of common mode failures due to maintenance or calibration errors), and that the beta-factor is assigned a value of 0.

4.2.6 Decomposing Blocks Into Modules

The decomposition of a block of medium or high complexity into simpler modules serves two main purposes: the identification of the modules where faults could lead to digital failures or digital CCFs, and the identification of module-specific failure modes of the block. This allows in turn the determination of corresponding defensives measures, the assessment of their coverage and effectiveness, and more realistic estimates of probabilities of digital failures and beta-factors. Decomposing blocks into modules won't be appropriate in every case; it depends on the specifics of the application.

Example 4-6a. Decomposing the Reactor Trip System (RTS) as Part of Failure Mode Analysis.

The RTS takes input from several process sensors to calculate the plant status with respect to plant safety limits. The only outputs are Boolean signals to actuate the reactor trip breakers. The RTS is implemented in the following manner:

- Process sensor measurements are input to digital process units that perform analog-to-digital conversions, engineering unit conversion, process calculations and output communication.
- The outputs of process units feed one or more simple voting units that perform input communication, voting logic, and digital-to-analog conversion and output to the reactor trip breakers.

Regardless of what digital failures are assumed to occur in the RTS logic, the output is either logic 1 or logic 0. Thus, for the purpose of failure modes identification, no decomposition into modules is necessary for the RTS.

However, for the purpose of evaluating defensive measures, it may be helpful to identify critical modules based on internal functionality. In this case, process units are decomposed into three modules, one for input conversion, one for digital logic processing, and one for output communication. The digital logic processing module is further decomposed into software modules that are evaluated per Table 4-2 (see Example 4-6b).

Example 4-6b. Decomposing the Software of the RTS Logic Processing Module to Evaluate Defensive Measures.

A "white-box" analysis of the software of the RTS logic processing module shows that it is composed of three main software sub-modules:

- The Operating System manages the hardware and provides all the generic services necessary for the functioning of the PLC (e.g., monitoring of hardware, handling of inputs, outputs, and exceptions).
- The Application Function Library provides a number of elementary functions to be used by applications (e.g., mathematical functions).
- The Application Software implements application specific logic processing.

The analysis also shows that:

- The Operating System functions cyclically in extremely stable conditions (static allocation of resources, very limited memory is kept from one cycle to the next, no management of date and time); in particular, it is not affected by plant conditions (no plant-related interrupts, transparent to input values).
- The Application Function Library is composed of small, simple, memoriless, well-verified software functions based on proven algorithms.
- The Application Software is generated automatically from the functional specification, using high quality, tried and tested tools.

It is concluded that:

- Because the Operating System repeats the same sequence of actions cycle after cycle, regardless of the plant status, it is essentially blind to plant transients and is therefore very unlikely to cause a digital CCF, either during a plant transient or during stand-by conditions, even in identical channels.
- Because of its simplicity, modularity, extensive testing and successful operating history, the Application Function Library is also very unlikely to cause digital failures.
- While the Application Software is relatively simple and is backed by a strong development process, it has little operating history. It is therefore concluded that the probability of digital failures and digital CCFs is driven by the likelihood of functional specification faults in the Application Software.

Sometimes it is useful to decompose blocks into functional modules to systematically identify and address internal failure modes that can have different system-level effects. This would typically be the case for blocks with more complex functionality than simple Boolean logic.

Example 4-7. Decomposing Blocks to Identify Internal Failure Modes - Safeguards Load Sequencer.

This single digital unit has two inputs ("Bus Voltage" and "SI (Safety Injection) Signal") and multiple outputs ("on/open" and "off/close" commands to safeguard pumps and valves) and is in charge of sequencing loads onto the diesel generators. In order to capture all the potential failure modes that may result from postulated internal failures, the system designer examines the logic of the sequencer. It can be decomposed into three different functional modules:

- "Undervoltage Detection" determines from the "Bus Voltage" input whether loss of voltage has occurred. If so, undervoltage load shedding occurs and an "Undervoltage" signal is transmitted to "Load sequencer."
- "SI Detection" determines from the "SI Signal" input whether an SI actuation has occurred. If so, SI load shedding occurs, and an "SI actuation" signal is transmitted to the "Load sequencer."
- "Load Sequencer" performs the load sequencer logic when it receives the "Undervoltage" and/or the "SI actuation" signals. The outputs are actuation signals to the safeguard components.

The importance of modeling these three functional modules is demonstrated by performing a failure analysis on the sequencer.

Failure Scenario 1: Postulated Failure in "SI Detection" - Assume a failure occurs in "SI Detection" such that the SI loads are not shed, but the "SI actuation" signal is transmitted to "Load Sequencer." The designer should demonstrate that the plant Unit Auxiliary Transformers (UATs) have adequate margin to handle the sequenced loads in addition to the load corresponding to the components that were not shed due to the postulated failure.

Failure Scenario 2: Postulated Failure in "Load Sequencer" - Assume an "Undervoltage" signal is detected, the undervoltage loads are shed and the feeder breakers receive an open command. After the diesel is running, a "diesel output breaker closed" signal and a "feeder breaker open" signal are received by the "Load Sequencer." Assume a failure occurs in "Loads Sequencer" such that the all undervoltage components are activated simultaneously. The diesel should be shown to have sufficient capacity to handle all those loads, or it should be shown that the diesel output breakers will be tripped with no resultant damage to the diesel. Controls should be available to the operator to manually shed the loads, close the diesel output breaker and sequence the necessary loads.

If the sequencer is modeled by only one block, the above consequences of postulated internal failure modes would not be identified. Arguments may be provided that these internal functional modules are not susceptible to digital CCFs due to the use of a rigorous software development process and the use of defensive measures. However, it is necessary to recognize that these detrimental failure modes potentially exist and need to be addressed.

4.3 Principles of Risk-Informed Regulation as They Apply to D3 Evaluations

The methods presented in this guideline adhere to the five principles of risk-informed regulation outlined in Regulatory Guide 1.174 (see Reference [2]). These principles are directed at assuring decisions are made using a blend of traditional engineering analyses with insights derived from PRA. The following summarizes the principles as they relate to risk-informed D3 evaluations:

1. The proposed change meets the current regulations.
   The plant will continue to meet regulatory criteria with respect to the single failure criterion and diversity in response to ATWS. The plant must still have features that address General Design Criteria with respect to protection system reliability, independence, and separation. The initiating events analyzed in the SAR will continue to be addressed. The risk-informed D3 evaluation addresses a beyond design-basis issue in the form of digital CCF. The capability of the plant to cope with conditions associated with design-basis events is not affected, and current regulations will therefore continue to be met.
2. The proposed change is consistent with the defense-in-depth philosophy.
   The risk-informed approaches described in this guideline are specifically directed at demonstrating adequate defense-in-depth. Defense-in-depth is addressed from two perspectives: 1) maintenance of fission product barriers, and 2) redundancy and diversity in maintaining adequate core cooling or preventing a significant release given the frequency of various challenges. The potential effects of digital CCFs are directly evaluated, as well as the potential effects of digital failures on indications and controls used for human actions that are credited in D3 evaluations. The PRA is used to demonstrate that changes in CDF and LERF are small. Independent of the PRA, a confirmatory review of defense-in-depth is performed consistent with the Reactor Oversight Process. Defense-in-depth therefore plays an integral role in the demonstration of adequate ability to cope with the effects of digital CCF when the evaluation is performed in accordance with this guideline.
3. The proposed change maintains sufficient safety margin.
   As the ability of the plant to mitigate the events analyzed in the SAR is preserved, and as the analysis of such events will still comply with acceptance criteria in the licensing basis, the margin of safety that exists for these events is maintained. This guideline introduces alternate methods for demonstrating adequate defense-in-depth when considering the potential for digital CCF. These alternate methods address beyond-design-basis conditions.
4. When proposed changes result in an increase in core damage frequency or risk, the increases should be small and consistent with the intent of the Commission's Safety Goal Policy Statement.
   Detailed guidance is provided in this document with respect to estimating the change in risk associated with digital CCF and in using Figures 3 and 4 of Regulatory Guide 1.174 to provide confirmatory assurance based on deterministic considerations. Documentation of the reasons for these quantitative results in terms of plant design features and operating characteristics is recommended.

5. The impact of the proposed change should be monitored using performance measurement strategies.
   Existing plant corrective action, maintenance rule and reporting programs govern documentation and response to any non-conformances that occur associated with the digital upgrade. Whether risk-informed or deterministic D3 evaluations are performed, monitoring of satisfactory operation of the upgrade is performed subsequent to its installation.

4.4 PRA Modeling for D3 Evaluation

Whether updating the PRA to reflect a digital upgrade or performing a risk-informed D3 evaluation, it is important to assure that the level of detail in the I&C modeling in the PRA reflects the functional impact of the digital equipment to be installed. Two approaches for assuring that the functional impact of the digital equipment is appropriately taken into account are:

1. Detailed modeling of the failure modes of the digital equipment and their effects on the plant systems that they support. This is a bottom up approach that may require detailed investigation of the failure mechanisms of the digital equipment with incorporation of mathematical models into the PRA to simulate the effects of these failures.
2. High level investigation of potential functional effects of digital failures, without modeling the specific mechanisms. This is a top down approach that takes advantage of the design of the plant systems supported by the digital equipment to determine where digital failures may be most important to safety.

Regardless of the approach taken, consideration should be given to incorporating into the PRA any digital failure modes that could disable equipment or operator actions that are credited in the PRA. The following discusses the pros and cons of the two approaches.

4.4.1 Detailed Modeling Approach

To implement the detailed modeling approach, the modeling of the digital system should include:

- Identification of the various failure modes of hardware and software components of the upgrade.
- Development of appropriate mathematical and logic models (e.g., Markov, dynamic fault trees, etc.) to simulate the occurrence of these failure modes.
- Assessment of the potential for these failure modes to cause loss of the functions associated with the mitigating systems for different accident sequence conditions.

The advantage of this approach is that the final logic models should most accurately reflect the effects of a spectrum of digital failure modes, demonstrating their likelihood and importance in an objective manner. Should a digital failure mode be discovered that has a significant effect on safety, the models would offer a variety of options to address the potential vulnerability without introducing unnecessary conservatisms. These options could range from additional "white-box" evaluation and testing of the digital equipment to changing the design of mitigating systems to accommodate the potential failure.

Disadvantages of the detailed modeling approaches are that techniques and data evaluation for this level of detail are still evolving. Utilities are implementing upgrades that may need to be designed and operational before the detailed analytical techniques for evaluating these types of failures are mature.

4.4.2 Super-Component Approach

This approach takes advantage of the fact that the functional impact of failures of plant I&C is currently reflected in the mechanical and electrical trains of equipment that make up the mitigating systems modeled in the PRA. To consider the effects of digital failures, it may only be necessary to incorporate super-components (i.e., events representing the failure of collections of components) into the PRA logic models at appropriate locations, effectively reflecting the loss of the key functions that the digital equipment supports. The super-component approach includes:

- Recognition of key functions credited in the PRA for mitigation of each accident sequence.
- Identification of plant systems that support each of these functions.
- Incorporation within each plant system of super-components that represent the failure of the system to perform the specified function.

In incorporating the primary effects of potential digital failures using the super-component approach, it is not likely that individual sensors, actuation channels, or divisions of logic will drive the reliability of the plant systems they control. Rather, in estimating the effects of digital failures, it is most important to assure that the super-components reflect inter and intra-system effects of these failures (beta-factors). In this regard, incorporation of super-components reflecting the common cause effects of digital equipment will capture the dominant effects of digital component failures.

The advantage of the super-component approach is that it is relatively easy to implement and is similar to the manner in which complex I&C systems are typically modeled in PRAs for the current generation of plants (e.g., for the reactor trip system). Functions that are important to managing safety as defined by the existing PRA can be used to focus the analysis.

A possible disadvantage of this approach is that it may lead to overly conservative assumptions in modeling the effects of functional I&C failures and in estimating the potential for these failures.

4.4.3 Data Assignment

Whether using detailed modeling or the super-component approach, it should be recognized that assignment of digital failure probabilities and beta-factors does not reflect the same considerations as for typical hardware. Random hardware failure probabilities are typically based on aging and wear-out of hardware components. Software does not wear out. It can however cause malfunctions by generating undesired responses to plant conditions. As noted in Section 2, digital failure probabilities and beta-factors should reflect:

- The potential for the digital equipment to encounter unanticipated conditions
- The potential for the digital equipment to respond incorrectly to anticipated conditions.
- The potential for the triggering conditions to affect multiple channels or systems concurrently.

Section 4.2 addresses the determination of the potential for these means of digital failure and digital CCF, including identification of defensive measures that are effective in avoiding or tolerating them.

For the purpose of performing a D3 evaluation, assignment of bounding values is appropriate. Where realistic values are selected, an assessment of the range of values that might be assigned should be performed to assess the impact of uncertainties (e.g., determine what combinations of digital failure probability, beta-factor and initiating event frequency will significantly alter the results).

When updating the PRA to reflect the digital upgrade, either the detailed or super-component approach to modeling the functional effects of the digital upgrade is applicable. However, realistic values for the probabilities of digital failure and the beta-factors should be assigned, as opposed to bounding values, so as not to inappropriately bias the PRA when it is used for other applications.

4.4.4 Addressing Uncertainties

Three types of uncertainties can influence the results of a PRA (see Regulatory Guide 1.174 (see Reference [2]):

1. Parametric uncertainties, i.e., uncertainties regarding failure probabilities, beta-factors and initiating events frequencies.
2. Modeling uncertainties, i.e., uncertainties in the deterministic behavior of systems and components, including success criteria, failure modes and their effects.
3. Completeness uncertainties: from a D3 evaluation perspective, these uncertainties result either from insufficient scope of modeling of I&C systems or from insufficient coverage of initiating events.

Whether using detailed modeling of the digital I&C or the super-component approach, acceptable methods of addressing these uncertainties for the purposes of D3 evaluations could include the following:

- Parametric uncertainties can be addressed either by using bounding values or by performing sensitivity studies.
- Modeling uncertainties can be addressed by taking a high level functional approach where important functions of plant systems are assumed to be affected adversely by digital failures. Thus, for D3 purposes, uncertainties associated with modeling assumptions are handled conservatively.
- Completeness uncertainties can be addressed by assuring that the model includes all potential failures of functions important for providing core cooling or preventing significant radiation release, for all initiating events modeled in the PRA, as well as location dependent initiators (such as internal fires and floods) and external events (such as seismic events).

4.4.5 Other Effects of Digital Upgrades

In incorporating the digital upgrade into the PRA models, other positive effects on the plant are worthwhile to consider, to the extent practical. For example:

- Reduction of initiating event frequencies. Often, upgrades will include balance of plant systems important to the operation of the plant. Replacement of single train analog controls with fault tolerant, self-monitoring equipment can reduce the expected frequency of initiating events associated with these systems.
- Removal of the contribution to failure from the analog I&C. While I&C does not typically dominate the reliability of the mitigating systems, a small reduction in their failure probabilities can be achieved by removing the logic being replaced from the model or setting its failure probability to zero.
- Credit for additional condition monitoring. Continuous monitoring of normally operating equipment may be a part of the upgrade and can have the beneficial effect of reducing the failure probability of monitored equipment below that of equipment with longer surveillance and maintenance intervals.

It is also recommended that potential negative effects of diverse backups added to mitigate digital CCFs be addressed realistically. For example, additional backups can be sources of:

- Spurious actuations that may increase frequencies for some initiating events.
- New failure modes.
- Single points of failure that may increase beta-factors.
- Modeling uncertainties.

4.5 Importance of Evaluating D3 Issues Early in a Modernization Program

There are a number of reasons why it is important to consider D3 evaluations as early as possible in the I&C modernization process:

- Results of D3 evaluations can feed back and impact the I&C design, regardless of which method is used to perform the evaluation.
- Upgrades that are planned and performed without any consideration of D3 issues can lead to the need for backups to be added later on that could have been avoided.

The best way to avoid unnecessary changes late in the program is to consider D3 issues and solutions at the beginning of the design process, when the initial architecture for the upgraded I&C systems is defined:

- Risk insights can be helpful in optimizing the architecture to get the most benefit (and least risk) from digital upgrades. Early consideration of the impact of digital systems on plant risk can be helpful in making design decisions on architecture and equipment selection. For example, digital systems are capable of performing multiple functions (combining functions on one processor or module that were previously performed using separate analog devices). Also, signals can be communicated from one system to another to enhance control functionality. However, risk evaluations may show that these types of combinations or interconnections introduce new failure modes that have not been previously analyzed, and which may increase risk. These risks should be considered before finalizing the design.
- Results of the D3 evaluations also can impact the control room human-system interface (HSI) design, plant operating procedures, and training. The reverse is also true – HSI design changes can impact the D3 evaluation. For example, implementation of soft controls as part of HSI modernization may eliminate manual controls and indications that later may be determined to be beneficial in addressing D3 issues. Without the controls, the D3 resolution could become more difficult. Or, if the controls are added back late in the design, it may be necessary to make compromises in the human factors aspects of the design to accommodate the back-fit.
- Consideration of D3 early in a project can help reduce the cost of addressing D3 during each successive modification (outage after outage) by providing an overall evaluation or template that can be re-used or simply referenced at each stage of the modification program (unless, of course, significant changes are made to the originally planned upgrades later in the program). At each stage in the project, the applicability of the overall D3 evaluation should be confirmed.
- Early evaluation of the impact of digital upgrades on plant risk and the corresponding changes that will be needed to the plant-specific PRA can help the plant later in keeping the PRA up-to-date, and using consistent methods for updating it to reflect digital implementations.

Sensitivity studies performed using representative plant PRAs have led to several important risk insights that should be considered in the early stages of a digital upgrade (see Reference [20]):

- The level of diversity and defense-in-depth in the plant design can have as much or greater impact on overall risk than the values assumed for P_{DF} and beta-factors – the change in plant risk may not be very sensitive to the specific values that are chosen.
- Where redundancy and diversity currently exist within the design of the mitigating systems for a given initiating event and have a significant impact on safety, it is important not to introduce new digital CCFs that are likely to adversely impact multiple mitigating functions.
- By the same token, introducing diversity into the I&C of a mitigating system where there is not comparable diversity in the mechanical and electrical equipment that it actuates is likely to have little beneficial impact on the overall reliability of the mitigating system, and may, in fact, reduce human reliability from training and familiarity issues.

Taking credit for operator action to mitigate certain initiating events can have a significant beneficial impact on risk. However, when this is done, it is important to ensure that the HSI the operators will need in order to perform the action will not be subject to the same failures that lead to the need for operator action.

4.6 Documentation and Licensing Submittals

Regardless of whether the licensee plans to submit a License Amendment Request (LAR), the results of the D3 evaluation should be documented. This section provides guidance on the types and scope of documentation that are appropriate. If a LAR is to be submitted, the detailed results need not necessarily be included in the LAR submittal for NRC review and approval; a simplified report that provides an overview of the evaluation and results should be adequate.

The documentation should follow accepted 10 CFR 50 Appendix B Design Control procedures so that the results of the evaluation are retrievable during the life of the plant.

4.6.1 Identification of Susceptibilities and Defensive Measures

Defensive measures credited as important in the D3 evaluation should be captured in the documentation of the initial acceptance for the digital equipment (essentially becoming part of its design-basis documentation). Then, when changes are made to the equipment while it is in service (e.g., software or hardware updates from the manufacturer), this information can be used as part of ensuring acceptability of the changes, i.e., ensuring that risk related to digital failures and digital CCFs is still adequately managed as maintenance updates are performed over time. The documentation should include sufficient information so that the following can be verified:

- The design elements susceptible to digital failures and their postulated failure mechanisms are identified correctly.
- The set of credited measures covers and provides an effective defense against the identified failure mechanisms.

- Each credited measure has been implemented correctly.

It should not be necessary to "re-open" the D3 evaluation every time maintenance is done on the digital equipment. Once the equipment is in service, the burden shifts to those routine activities performed when changes are made to ensure that the equipment maintains consistency with the original basis for its acceptance.

4.6.2 Extended Deterministic Method

The results of each of the steps of the Extended Deterministic Method as discussed in Section 3.2 should be documented. The primary areas that should be documented include the following.

- If a D3 evaluation is not required per the conditions of Section 2.1, a justification should be provided as to why each of the specified conditions do not apply to the upgrade.
- A concise simplified diagram should be generated that documents the design upon which the D3 evaluation was based. The detailed functional diagram from which the simplified diagram was based should also be included or referenced.
- Using the simplified diagram, a record should be kept of the postulated digital CCFs that were evaluated. As part of the record, the functions that are potentially degraded by the postulated digital CCFs should also be documented.
- A table should be generated that identifies the primary and backup protection functions assumed in the plant SAR accident analyses. Appropriate references to the SAR should be documented.
- The results of the comparison between the protection functions degraded by a postulated digital CCF and the protection functions assumed for each initiating event analyzed in the SAR should be documented.
- If one or more SAR events are identified in which both the primary and backup mitigating functions are degraded, the assumptions, analysis methods, and results of the best-estimate analyses of the events should be documented. Also, a description of the coping capability that is credited and appropriate justification should be included.
- If a risk-informed method is used for specific events (see Section 3.2), follow the documentation guidance given below for that method, focusing only on the specific events considered in the risk-informed analysis.

4.6.3 Risk-Informed Methods

The level of documentation useful for a risk-informed evaluation depends on the complexity of the analysis and the extent to which the models and various elements of the PRA were used in performing the evaluation. In this regard, the documentation for a risk-informed digital upgrade evaluation will depend on whether the Standard or the Simplified Risk-Informed Method was used.

Only a limited amount of documentation is needed to support a Simplified Risk-Informed evaluation. This evaluation requires input from only a few elements that make up the PRA (e.g.,

initiating events and frequencies, basis for credit for operator actions, basis for conditional failure probabilities for mitigating systems and conditional LERF). Those inputs, the estimates of the change in CDF and LERF that are calculated, and the comparison to Regulatory Guide 1.174 (see Reference [2]) acceptance guidance should be documented.

A detailed use of the PRA as outlined in the Standard Risk-Informed Method would result in correspondingly more detailed documentation. Beyond that described for the Simplified Risk-Informed Method, the documentation should include the modification and quantification of system models and accident sequence quantification.

When documenting the output of the evaluation, a review of accident sequence quantification results is recommended to ensure that they can be explained from an engineering context, with a focus on the following questions (which apply whether the Standard or the Simplified Risk-Informed Method is used):

- Which initiating events dominate the change in CDF and LERF, and why?
- What accident sequence types and initiators are not significantly affected? What limits the effect of the upgrade on these sequences?
- For the dominant contributors to ΔCDF and ΔLERF, what design features of the upgrade and/or the plant keep these changes small?
- To what extent do operator actions and recoveries play a role in keeping the risk associated with digital CCF small?
- How has the evaluation addressed the five principles of Regulatory Guide 1.174? (See Section 4.3).

When documenting the D3 evaluation, the technical adequacy of the information from the PRA should be reviewed. Several methods of accomplishing this review are available (see References [28], [29], [30]). The extent of the review is dependent on the degree to which the PRA was used as input to the evaluation.

4.6.4 Confirmatory D3 Review

The confirmatory D3 review should be documented in a manner consistent with the Significance Determination Process (see Section 3.5). This should include documentation of the defense-in-depth matrix used and where each event falls on the matrix.

5
REFERENCES AND DEFINITIONS

5.1 Bibliography

1. Branch Technical Position HICB-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems."
2. Regulatory Guide 1.174, Revision 1, "An Approach for Using Probabilistic Risk Assessment in Risk-informed Decisions on Plant-Specific Changes to the Licensing Basis," November 2002.
3. EPRI 1002833, "Guideline on Licensing Digital Upgrades TR-102348 Revision 1 NEI 01-01 – A Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule," March 2002.
4. NRC Regulatory Issue Summary 2002-22, "Guideline on Licensing Digital Upgrades: EPRI TR-102348 Revision 1, NEI 01-01: A Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule," November 2002.
5. NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," December 1994.
6. NUREG 0711 Revision 1, "Human Factors Engineering Program Review Model."
7. Safety Requirements Memorandum, "SECY-93-087: Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," July 1993.
8. Code of Federal Regulations, Title 10, Part 100: "Reactor Site Criteria."
9. Code of Federal Regulations, Title 10, Part 50.59: "Changes, Test and Experiments."
10. Chris Garrett & George Apostolakis, "Context in the Risk Assessment of Digital Systems," in Risk Analysis, Vol. 19, N° 1, 1999.
11. ASME RA-S-2002, Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications.
12. ANS N18.2-1973, "Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants."
13. Code of Federal Regulations, Title 10, Part 50.62, "Requirements for Reduction of Risk From Anticipated Transients Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants."
14. NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, Chapter 7, Instrumentation and Controls."
15. NEI 96-07 Revision 1, "Guidelines for 10 CFR 50.59 Implementation," November 2000.

16. IAEA NS-G-1.3, "Instrumentation and Control Systems Important to Safety in Nuclear Power Plants – Safety Guide."
17. IEC 61226, "Nuclear Power Plants - Instrumentation and Control Systems Important for Safety – Classification," 1993.
18. IEC 60880, "Software for computers in the safety systems of nuclear power stations," 1986.
19. IEC 60987, "Programmed Digital Computers Important to Safety for Nuclear Power Stations," November 1989.
20. D.P. Blanchard & R.C. Torok, "A Risk-Informed Approach to Evaluating Digital Upgrades," 13th Annual Joint ISA POWID/EPRI Control & Instrumentation Conference, June 2003.
21. IEEE Std 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."
22. EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," October 1996.
23. Generic Letter 88-20 "Independent Plant Examination for Severe Accident Vulnerabilities," USNRC, November 23, 1988.
24. "Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities," Federal Register Vol. 60 pg. 42622, August 16, 1995.
25. SECY-99-007A, "Recommendations for Reactor Oversight Process Improvements (Follow-up to SECY-99-007)," March 1999.
26. IEEE Std 7-4.3.2-2003 "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations."
27. Lutz, Robyn R., "Analyzing Software Requirements Errors in Safety-Critical, Embedded Systems," Software Requirements Conference, IEEE, January 1992.
28. NEI 00-02, "Probabilistic Risk Assessment (PRA) Peer Review Process Guidance," Rev. A3, March 2000.
29. ASME RA-S-2002, "Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications," April 2002.
30. Regulatory Guide 1.200, "An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities," February 2004.

5.2 Glossary

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 [ ].

Accident sequence. A representation in terms of an initiating event followed by a combination of system, function, and operator failures or successes, of an accident that can lead to undesired consequences, with a specified end state (e.g., core damage or large early release). An accident sequence may contain many unique variations of events (minimal cut sets) that are similar. (See Reference [11])

Application software. Part of the software that performs the tasks related to the process being controlled rather than to the functioning of the system [adapted from IEC 61513].

Best-estimate analysis. Analysis that uses realistic inputs and assumptions – this is in contrast to the plant licensing basis safety analysis, which uses conservative values for inputs and makes worst-case assumptions. Best-estimate analysis is intended to provide a realistic, as opposed to conservative, estimate of what the actual behavior of the plant will be for a given scenario.

Beta-factor. Assuming that a system or equipment has already failed, the conditional probability of concurrent failure of a redundant system or equipment (identical or diverse).

Block. The smallest portion of the system for which it can be credibly assumed that internal failures, including the effects of software errors, will not propagate to other equipment. (See Reference [5])

Channel. An arrangement of components and modules as required to generate a single protective action signal when required by a generating station condition. A channel loses its identity where single protective action signals are combined. (See Reference [21])

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 redundant systems. CCFs can occur due to design, operational, environmental, or human factor initiators. CCFs 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 redundant systems using the same equipment, regardless of whether they are common mode or common cause, the two terms are used interchangeably in this document. (See Reference [3])

Core damage. Uncovery and heatup of the reactor core to the point at which prolonged oxidation and severe fuel damage is anticipated and involving enough of the core to cause a significant release. (see Reference [11])

Core Damage Frequency (CDF). Expected number of core damage events per unit time. (See Reference [11])

Defense-in-depth. A concentric arrangement of protective barriers or means, all of which must be breached before a hazardous material or dangerous energy can adversely affect human beings or the environment. For instrumentation and control systems, the application of the defense in depth concept includes the control system; the reactor trip or scram system; the Engineered Safety Features Actuation System (ESFAS); and the monitoring and indicator system and operator actions based on existing plant procedures. The echelons may be considered to be concentrically arranged in that when the control system fails, the reactor trip system shuts down

reactivity; when both the control system and the reactor trip system fail, the ESFAS continues to support the physical barriers to radiological release by cooling the fuel, thus allowing time for other measures to be taken by reactor operators to reduce reactivity. (see Reference [5])

Dependability. As used in this document, a broad concept incorporating various characteristics of digital equipment, including reliability, safety, availability, maintainability, and others. (See Reference [3])

Design-Basis Event. Postulated events that are a part of the Safety Analysis used in the design to establish the acceptable performance requirements for the structures, systems, and components.

Digital Common Cause Failure (digital CCF). A systematic common cause failure resulting from a design fault in a digital system or component (e.g., a design error in the software or software-hardware interaction).

Digital upgrade. A modification to a plant system or component which involves installation of equipment containing one or more computers. 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). (see Reference [3])

Diversity. Existence of two or more different ways or means of achieving a specified objective.

Failure. Termination of the ability of a functional unit to perform a required function

Failure probability. The likelihood that an SSC (System Structure or Components) will fail to operate upon demand or fail to operate for a specific mission time. (see Reference [11])

Fault. A defect that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function when subjected to a particular set of normal or abnormal operating conditions.

Fault tree. A deductive logic diagram that depicts how a particular undesired event can occur as a logical combination of other undesired events. (See Reference [11])

Firmware. Software that resides in read-only memory. An example is programmable read-only memory (PROM). (See Reference [3])

Functional accident sequence type. A grouping of the accident sequences developed for the plant-specific PRA into bins that reflect one or more functions that must fail or otherwise be unavailable in order to get into a condition in which inadequate core cooling or significant releases are occurring.

Functional mistake. An error made in the functional specification of an I&C system that is caused by an insufficient or incorrect understanding of the operational environment of the system and of the functions to be performed by the system (see also Technical mistake).

Functional specification. A document that specifies the functions that a system or component must perform. [IEEE 610.12.1990]

Human factors - A body of scientific facts about human characteristics. The term covers all biomedical, psychological, and psycho-social considerations; it includes, but is not limited to, principles and applications in the areas of human factors engineering, personnel selection, training, job performance aids, and human performance evaluation (see "Human factors engineering").(See Reference [6])

Human Factors Engineering (HFE) - The application of knowledge about human capabilities and limitations to plant, system, and equipment design. HFE ensures that the plant, system, or equipment design, human tasks, and work environment are compatible with the sensory, perceptual, cognitive, and physical attributes of the personnel who operate, maintain, and support it (see “Human factors”). (See Reference [6])

Human-System Interfaces (HSIs) - A human-system interface (HSI) is that part of a plant system through which personnel interact to perform their functions and tasks. Major HSIs include alarms, information displays, controls, and procedures. Use of HSIs can be influenced directly by factors such as: (1) the organization of HSIs into workstations (e.g., consoles and panels); (2) the arrangement of workstations and supporting equipment into facilities such as a main control room, remote shutdown station, local control station, technical support center, and emergency operations facility; and (3) the environmental conditions in which the HSIs are used, including temperature, humidity, ventilation, illumination, and noise. HSI use can also be affected indirectly by other aspects of plant design and operation such as crew training, shift schedules, work practices, and management and organizational factors. [Adapted from 6]

Initiating Event (IE). Any event either internal or external to the plant that perturbs the steady state operation of the plant, if operating, thereby initiating an abnormal event such as transient or LOCA within the plant. Initiating events trigger sequences of events that challenge plant control and safety systems whose failure could potentially lead to core damage or large early release. (See Reference [11])

I&C architecture. Organizational structure of the I&C systems of the plant which are important to safety. [IEC 61513]

I&C platform. Set of hardware and software components that may work co-operatively in one or more defined architectures (configurations) [IEC 61513]

I&C system. System, based on electrical and/or electronic and/or programmable electronic technology, performing I&C functions as well as service and monitoring functions related to the operation of the system itself.

Large early release. The rapid, unmitigated release of airborne fission products from the containment to the environment occurring before the effective implementation of off-site emergency response and protective actions. (See Reference [11])

Large Early Release Frequency (LERF). Expected number of large early releases per unit time. (See Reference [11])

Operating system. The machine resident software that enables a computer to function. Without it, application programs could not be loaded or run

Probabilistic Risk Assessment (PRA). A qualitative and quantitative assessment of the risk associated with plant operation and maintenance that is measured in terms of frequency of occurrence of risk metrics, such as core damage or a radioactive material release and its effects on the health of the public (also referred to a probabilistic safety assessment, PSA). (See Reference [11])

Random failure. Failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware

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. (See Reference [3])

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

Risk. Probability and consequences of an event, as expressed by the "risk triplet" that is the answer to the following three questions (1) What can go wrong? (2) How likely is it? (3) What are the consequences if it occurs? (See Reference [11])

Software. Computer programs, procedures, and possibly associated documentation and data pertaining to the operation of a computer system. This includes software that is implemented as firmware. (See Reference [3])

Super-component. An event within a logic model that represents the failure of a collection of components.

Susceptibility. Quality of being sensitive to an extraneous agent or effect. For the purposes of this document, susceptible means that digital CCFs are possible at the component, system or multiple system level. However, such failures do not necessarily affect risk significantly at the plant level. (this is in contrast to use of "vulnerability").

System. A collection of equipment that is configured and operated to serve some specific plant function(s) (e.g., provides water to the steam generators, sprays water into the containment, injects water into the primary system).

Technical mistake. An error made in the functional specification of an I&C system, where the analyst has an appropriate understanding of the operational environment of the system and of the functions to be performed by the system, but provides an incorrect or incomplete expression of these functions (see also Functional mistake).

Train. A collection of equipment that is configured to provide a specific function or signal and is a sub-set of an overall system that is designed to accomplish that particular function or signal.

Vulnerability. Quality of being open to attack or damage. In this document, vulnerability is used to refer to increased risk at the plant level due to digital CCF (this is in contrast to the use of "susceptibility").

"White-box." System or component whose internal contents or implementation are known. [IEEE 610.12.1990]

5.3 Abbreviations and Acronyms

AFW	Auxiliary Feed Water
ALWR	Advanced Light Water Reactor
ANS	American Nuclear Society
ANSI	American National Standards Institute
ASME	American Society of Mechanical Engineers
ATWS	Anticipated Transient Without Scram
BTP	Branch Technical Position
CCF	Common Cause Failure
CDF	Core Damage Frequency
CFR	Code of Federal Regulations
CMF	Common Mode Failure
D3	Diversity & Defense-in-Depth
EPRI	Electric Power Research Institute
ESFAS	Engineered Safety Features Actuation System
ESW	Essential Service Water
HSI	Human-System Interface
I&C	Instrumentation & Control
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineer
IPE	Individual Plant Evaluation
IAEA	International Atomic Energy Agency
LAR	License Amendment Request
LBLOCA	Large-Break Loss Of Coolant Accident
LERF	Large Early Release Frequency
LOCA	Loss Of Coolant Accident
NEI	Nuclear Energy Institute
NRC	Nuclear Regulatory Commission
NUREG	Nuclear Regulation
P_{DF}	Probability of Digital Failure
P_F	Probability of Failure

PORV	Power Operated Relief Valve
PRA	Probabilistic Risk Assessment
RTS	Reactor Trip System
SAR	Safety Analysis Report
SDP	Significance Determination Process
SI	Safety Injection

WARNING: This Document contains information classified under U.S. Export Control regulations as restricted from export outside the United States. You are under an obligation to ensure that you have a legal right to obtain access to this information and to ensure that you obtain an export license prior to any re-export of this information. Special restrictions apply to access by anyone that is not a United States citizen or a Permanent United States resident. For further information regarding your obligations, please see the information contained below in the section titled "Export Control Restrictions."

Export Control Restrictions

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

About EPRI

EPRI creates science and technology solutions for the global energy and energy services industry. U.S. electric utilities established the Electric Power Research Institute in 1973 as a nonprofit research consortium for the benefit of utility members, their customers, and society. Now known simply as EPRI, the company provides a wide range of innovative products and services to more than 1000 energy-related organizations in 40 countries. EPRI's multidisciplinary team of scientists and engineers draws on a worldwide network of technical and business expertise to help solve today's toughest energy and environmental problems.

EPRI. Electrify the World

Program: 1002835

Nuclear Power

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