EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Modeling of Digital Instrumentation and Control in Nuclear Power Plant Probabilistic Risk Assessments

2012 TECHNICAL REPORT

Modeling of Digital Instrumentation and Control in Nuclear Power Plant Probabilistic Risk Assessments

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

EPRI Project Manager
R. Torok

ELECTRIC POWER RESEARCH INSTITUTE

3420 Hillview Avenue
Palo Alto, CA 94304-1338
USA

PO Box 10412
Palo Alto, CA 94303-0813
USA

800.313.3774
650.855.2121

askepri@epri.com

www.epri.com

1025278

Final Report, July 2012

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

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

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

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

REFERENCE HEREIN TO ANY SPECIFIC COMMERCIAL PRODUCT, PROCESS, OR SERVICE BY ITS TRADE NAME, TRADEMARK, MANUFACTURER, OR OTHERWISE, DOES NOT NECESSARILY CONSTITUTE OR IMPLY ITS ENDORSEMENT, RECOMMENDATION, OR FAVORING BY EPRI.

THE FOLLOWING ORGANIZATION, UNDER CONTRACT TO EPRI, PREPARED THIS REPORT:

Applied Reliability Engineering, Inc.

Électricité de France (EDF)—R&D

THE TECHNICAL CONTENTS OF THIS DOCUMENT WERE **NOT** PREPARED IN ACCORDANCE WITH THE EPRI NUCLEAR QUALITY ASSURANCE PROGRAM MANUAL THAT FULFILLS THE REQUIREMENTS OF 10 CFR 50, APPENDIX B AND 10 CFR PART 21, ANSI N45.2-1977 AND/OR THE INTENT OF ISO-9001 (1994). USE OF THE CONTENTS OF THIS DOCUMENT IN NUCLEAR SAFETY OR NUCLEAR QUALITY APPLICATIONS REQUIRES ADDITIONAL ACTIONS BY USER PURSUANT TO THEIR INTERNAL PROCEDURES.

NOTE

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

Acknowledgments

The following organization, under contract to the Electric Power Research Institute (EPRI), prepared this report:

Applied Reliability Engineering, Inc.
3428 Balboa St.
San Francisco CA 94121

Principal Investigator
D. Blanchard

Électricité de France (EDF)—R&D
6, quai Watier
78400 Chatou
France

Principal Investigator
T. Nguyen

This report describes research sponsored by EPRI.

The project team would like to acknowledge the contributions of Bob Enzinna, of AREVA, Inc., as key portions of the technical approach are based on his work analyzing operating plant upgrades and the U.S. EPR design, and in support of a Nuclear Energy Institute (NEI) effort that addressed technical and regulatory issues regarding modeling of digital instrumentation and control in probabilitistic risk assessment.

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

Modeling of Digital Instrumentation and Control in Nuclear Power Plant Probabilistic Risk Assessments. EPRI, Palo Alto, CA: 2012. 1025278.

Abstract

Probabilistic risk assessment (PRA) typically models hardware components in terms of their failure probability and the effects that any given component failure has on the system it resides in. Digital systems, which include both hardware and software, bring new modeling challenges: determination of the appropriate level of detail to use in the logic models, and estimation of failure rates for software components. Failure probabilities for hardware are typically based on operating experience with component aging and wear-out. But software does not wear out; faults that create problems later are basically designed in. As a result, traditional methods for estimating hardware failure probabilities are difficult to apply to digital systems. There are currently no generally accepted methods for determining failure probabilities or the appropriate level of detail for digital systems.

This report from the Electric Power Research Institute (EPRI) describes a practical approach for incorporating digital instrumentation and control (I&C) system models in nuclear power plant probabilistic risk assessments. It addresses level-of-detail questions and proposes a method for estimating digital system failure rates. The guidance in the report focuses on recognizing the context of the I&C within the overall plant design, in particular with respect to failure modes of the electrical and mechanical equipment that it actuates and controls, as well as on accounting for common design practices and processes implemented by designers and owners that are intended to ensure the reliability of critical digital systems in the form of defensive measures.

The report overviews a nine-step process for modeling and quantification of digital I&C in PRA; introduces key terms and definitions related to the design of digital systems; discusses digital I&C logic models and their integration into a PRA; and describes the estimation of failure rates and probabilities of digital I&C components, including software.

Keywords

Instrumentation and control   I&C
Probabilistic risk assessment   PRA
Digital systems   Modeling

Table of Contents

List of Figures

List of Tables

Section 1: Introduction and Purpose

The purpose of this report is to describe methods for incorporating digital instrumentation and control (I&C) system models in nuclear power plant probabilistic risk assessments (PRA). The report focuses on the modeling of digital I&C for mitigating systems credited in the PRA, generally consisting of the plant protection system (engineered safety features actuation (ESFAS) and reactor trip systems (RTS)) and selected balance of plant systems with relatively simple control and feedback characteristics. Guidance is provided for two aspects of digital I&C modeling in PRA: determination of the appropriate level of detail needed in developing the logic models and estimation of failure rates for the purpose of quantification of the models.

Modeling of digital I&C in a nuclear power plant PRA can be accomplished using many of the same methods used to model analog I&C. This is due to the fact that components making up digital I&C perform many of the same functions as their analog counterparts (e.g., sensors, signal processors, voting and actuation devices) a difference being that a subset of these functions may be accomplished by different component types (e.g., processors as opposed to mechanical components such as relays or signal converters). The significant change between modeling of digital vs. analog systems in nuclear power plant PRA is the inclusion of software and its failure modes (see Sections 4 and 5). Without considering the software, the modeling of digital I&C hardware is a well-understood and mature process.

The methods discussed in this report are intended for use in application of PRA at both current plants, in upgrading to digital systems, as well as for the design and licensing of new plants. The proposed methods are directed at producing realistic results, endorse bounding techniques where information may not be available or is uncertain, and demonstrate by means of sensitivity analysis, the degree to which plant risk is sensitive to digital I&C reliability, including digital common cause failure (CCF).

It is not the intent of this methodology to achieve precision in the modeling and quantification of digital instrumentation and controls in PRA. Rather the objective of the methodology is to reinforce the need to consider 1) the context of the digital I&C being modeled with respect to the overall plant design and 2) the design practices and defensive measures that are common in the development, installation and operation of digital systems.

1.1 Context

Sensitivity studies have been performed by the reactor vendors [32, 33] and EPRI [1, 2, 3] to investigate the potential value of defense-in-depth and diversity in addition to high quality, to provide assurance that the potential for digital failure has been adequately addressed.. These studies demonstrate that three factors principally determine the degree to which digital I&C drives risk in a nuclear power plant PRA[1]:

- Reliability of the digital I&C systems (i.e., failure probability)
- The potential for intra-system failures (including dependencies and CCF)
- Defense-in-depth and diversity in the digital I&C as it relates to that of the mechanical and electrical systems into which the I&C is installed

By recognizing the context of the I&C within the plant design as a whole and maintaining the existing defense-in-depth and diversity of the systems being controlled by the digital I&C (that is, to the extent practical, not introducing significant common cause failures between redundant functions and systems that are diverse from a mechanical and/or electrical perspective [3]) potential key contributors to risk can be identified and managed more effectively.

1.2 Design Practices

High quality software, hardware and overall design reduce the potential for failure of digital I&C systems. In addition, defense-in-depth and diversity are key elements to providing evidence as to whether or not the potential for digital failures is a significant contributor to risk. The designers of digital I&C systems meet and often exceed the quality and defense-in-depth and diversity requirements of industry consensus design standards and practices.

In selecting methods for modeling of digital I&C in PRA, it is important to recognize not only the effects of defense-in-depth and diversity, but also the defensive measures that are typically applied to important digital systems by the designers to improve dependability [16], including those that go beyond assuring the quality of the software and hardware. Examples include use of watchdog timers and data validation routines that help protect against types of software faults, even when the specific errors have not been identified.

This report outlines an approach to digital I&C modeling in PRA that is intended for use in assessing the potential risks associated with digital I&C failures and the degree to which they have been addressed. The report emphasizes the need to consider both context and design practices and other defensive measures used in design, installation, operation and maintenance of these systems. Where the risk associated with digital failure is shown to be low primarily due to plant design features outside the digital system, then the PRA is

[1] Digital reliability and CCF, the first two bullets, are influenced to a considerable degree by design practices. The third bullet and shared dependencies from the second bullet, are determined by the context of the digital systems with respect to the rest of the plant design.

not sensitive to the digital system modeling, and the level of detail used in modeling the digital system is adequate.

This report is organized as follows:

Section 2 provides an overview of a nine step process for modeling and quantification of digital I&C in PRA.

Section 3 provides an introduction to key terms and definitions related to the design of digital systems that are important to their effective and efficient modeling in PRA.

Section 4 is directed at development of digital I&C logic models themselves and their integration into the PRA.

Section 5 focuses on the estimation of failure rates and probabilities of digital I&C components (including software).

Section 2: Digital I&C Modeling Process

2.1 Overview

The process described in this report for determining the level of detail needed in digital I&C models and developing digital system reliability estimates for use in a PRA consists of nine steps as shown in Figure 2-1. The process involves a confluence of I&C and PRA knowledge to identify and properly apply relevant information from both disciplines. Consistent with industry and regulatory guidance [4, 5] as well as consensus standards [6], the level of detail needed in modeling digital I&C in PRA is application-specific and depends on the sensitivity of the PRA results to the specific modeling choices. Hence, the process pays special attention to determining these sensitivities.

Figure 2-1 organizes the modeling steps and supporting activities in three columns to show which activities rely primarily on PRA expertise, which rely primarily on I&C expertise, and which need a collaborative effort. In addition to being able to build models and perform PRA analysis, the PRA specialist determines which plant functions need to be considered for potential interactions with I&C. The I&C specialist determines how potential I&C failures and misbehaviors might affect the plant functions modeled in the PRA and what protective mechanisms are in place that might affect the likelihood or consequences of an I&C related mishap. High level descriptions of the nine steps follow.

> Step 1 – Define I&C Architecture and systems/components modeled in PRA that are supported by the I&C – PRA and I&C specialists work together to determine what plant systems and components modeled in the PRA might be affected by the digital I&C under consideration and what portions of the I&C system will need to be modeled.
>
> Step 2 – Identify I&C failure modes and map failure effects to component failure modes modeled in the PRA – PRA and I&C specialists work together to identify the effects of digital I&C failures and misbehaviors at the level of the plant systems modeled in the PRA. Steps 1 and 2 define the scope of the analysis.
>
> Step 3 – Identify potential digital CCF susceptibilities - Inter- and intra-system effects of I&C failures and misbehaviors are examined to identify potential digital CCFs that may need to be added to the PRA model.

Step 4 – Develop PRA model with simplified treatment of digital I&C – The simplified model uses high level events and “super-components’ for the I&C failure effects and is used in Step 5 to assess relative importance of the digital system failures.

Step 5 – Estimating the sensitivity of the results of the PRA to digital I&C failures. – Use the simplified model from Step 4 in sensitivity studies to identify digital systems/components to which the results of the PRA are not sensitive and those digital system/components that may need detailed treatment.

Step 6 – Incorporate I&C modeling detail into the PRA based on Step 5 results – The PRA specialist adds detail to the model commensurate with the sensitivity of PRA results to the effects of the I&C and its failure.

Step 7 – Estimate digital system/component failure probabilities – The I&C specialist uses detailed digital system design information (e.g., failure mechanisms, defensive design measures) to develop reasonable parameter estimates for use in PRA given the sensitivity of PRA results to the effects of the I&C and its failure.

Step 8 – Regenerate the PRA results with final digital systems/components modeling – The PRA specialist uses the Step 6 and 7 outputs to generate PRA results and sensitivity studies that include the effects of digital system failures and misbehaviors on the plant.

Step 9 – Review/confirm PRA results, sensitivities, and insights – The PRA and I&C specialists jointly review the new PRA results to confirm that they are understood and reasonable, and to develop corresponding recommendations for plant design and operation considerations.

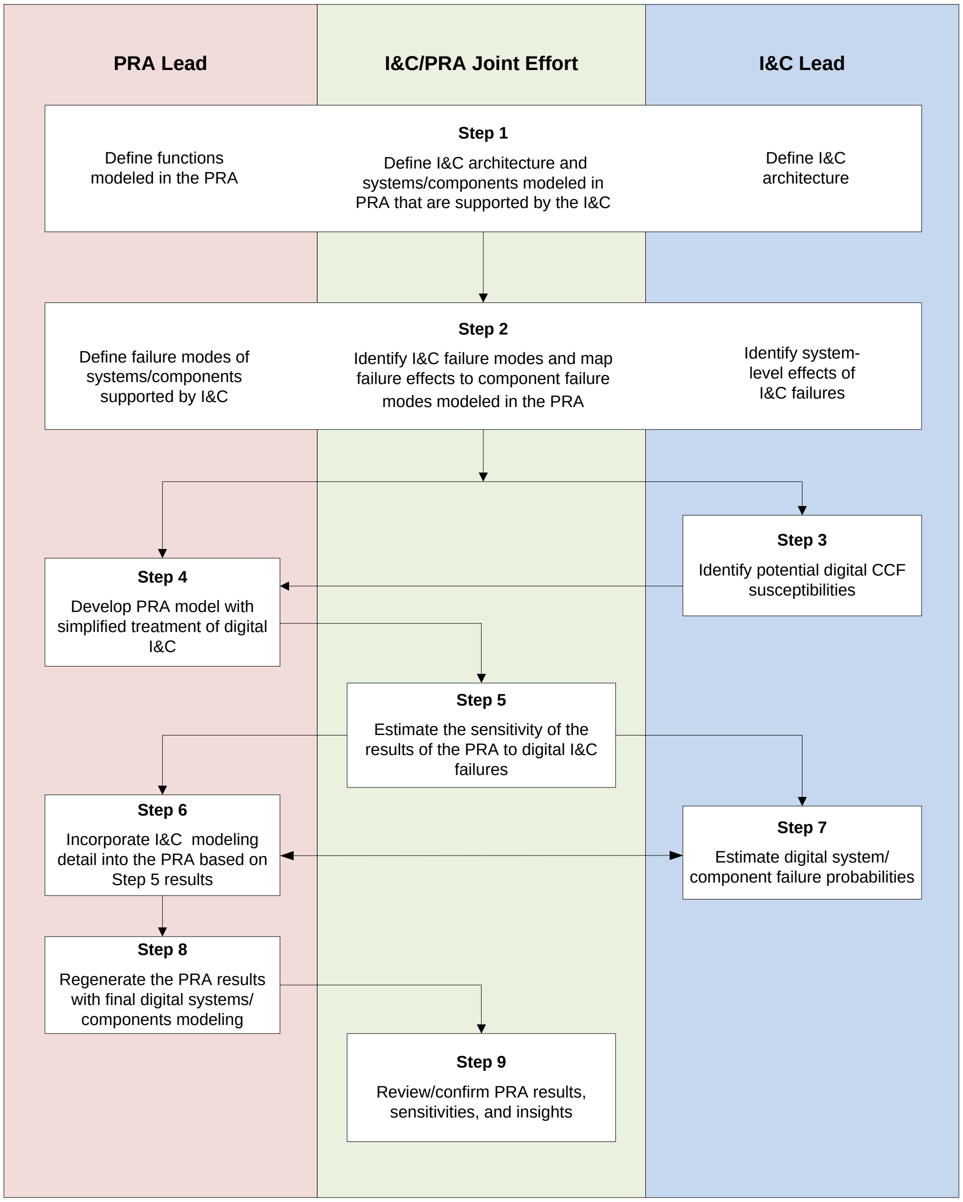

PRA Lead
I&C/PRA Joint Effort
I&C Lead
Step 1
Define functions modeled in the PRA
Define I&C architecture and systems/components modeled in PRA that are supported by the I&C
Define I&C architecture
Step 2
Define failure modes of systems/components supported by I&C
Identify I&C failure modes and map failure effects to component failure modes modeled in the PRA
Identify system-level effects of I&C failures
Step 3
Identify potential digital CCF susceptibilities
Step 4
Develop PRA model with simplified treatment of digital I&C
Step 5
Estimate the sensitivity of the results of the PRA to digital I&C failures
Step 6
Incorporate I&C modeling detail into the PRA based on Step 5 results
Step 7
Estimate digital system/ component failure probabilities
Step 8
Regenerate the PRA results with final digital systems/ components modeling
Step 9
Review/confirm PRA results, sensitivities, and insights

Figure 2-1
Process for Modeling Digital I&C in PRA

2.2 Detailed Process Description

This section provides a detailed description and discussion of each of the nine steps described above.

Step 1: Define I&C Architecture and systems/components modeled in PRA that are supported by the I&C

The first two steps in the process of developing digital I&C logic models in PRA are a joint effort by both I&C and PRA personnel. It is 'top down' in its approach, familiarizing PRA analysts with the overall architecture of the I&C and introducing I&C personnel to the functions and systems credited in the PRA.

In determining what to include in the PRA logic, I&C personnel provide an understanding of the spectrum of capabilities that a given digital system provides. Not all of these capabilities are considered in the PRA and it is the purpose of this initial step to focus follow-on efforts to just those aspects of the I&C design that support functions and systems modeled in the PRA.

I&C personnel may begin with an overview of the I&C architecture. For plant wide digital designs, this may include everything from monitoring and control of the plant and its systems to I&C logic for automatic initiation and control of safety-related and non-safety-related systems, including process interfaces. PRA analysts bring to the table knowledge of what safety functions and systems, including support systems, are credited in preventing core damage and significant releases. Much of what is different between these two sets of functions is an indication of what portions of the digital system can be set aside early in the modeling process. Overlaps identify plant functions, mitigating systems and components on which the digital I&C modeling process may wish to focus.

The suggested initial step in the process of modeling digital I&C in PRA is to identify plant mitigating systems, support systems and associated components included in the PRA that may be initiated or controlled by digital I&C. Note that the functions, systems and components that are being identified are not parts of the digital system. In this regard, little knowledge of the detailed design of the digital system is needed for these first few steps – only what plant systems the digital systems in question are intended to support.

It also is recognized that there are initiating events that could be triggered by failures or spurious actuations of particular digital systems. Once again, knowledge of the actuation and control functions by the I&C personnel provide indication of what operating or standby systems may be affected by such actuations. PRA personnel have an understanding of the various categories of initiating events that were developed in the PRA. A comparison of these two aspects of the effects of digital I&C on plant operating and standby systems can provide justification for eliminating some spurious operations from consideration at this early stage and focusing the modeling effort on just those actuations that may impact the outcome of the PRA.

Step 2: Identify I&C failure modes and map failure effects to component failure modes modeled in the PRA

Having identified the plant systems and components that a given digital system can affect, an understanding of the failure modes of interest for the electrical/mechanical equipment within these systems that are modeled in the PRA is essential to determining what failure modes are of interest at the digital system level for those digital systems that support these components. Having this understanding, it may be possible to screen out a number of failure modes at the digital system level and focus on only those that can significantly affect the PRA results.

Again, the PRA analysts can provide a list of failure modes considered in the PRA for each of the systems and components that were identified in the first step. I&C personnel have an understanding of potential digital system failure modes and effects and have access to failure modes and effects analyses developed in the design of the digital system. Those failure modes of plant electrical or mechanical components modeled in the PRA that cannot be caused by the I&C can be used to screen failure modes at the digital system level from further consideration. Similarly, digital I&C related failure modes that cause plant system and components to perform their intended functions as modeled in the PRA can be screened. At the same time, potential digital system effects known to I&C personnel that may not have been considered in the PRA can be added to the models.

Example components and their failure modes that are modeled in a PRA would be ECCS valves failing to open or breakers to injection pumps failing to close. The digital system failure modes of interest would include those that result in no actuation signal or no output. If, for the accident sequences in question, the actuation signal were not required for a significant period after the occurrence of plant conditions triggering the action (on the order of several minutes, for example), then consideration of failure modes such as delayed output may not be necessary. In addition, spurious actuation of the digital system may result in operation of the mitigating system. If this were shown to have adverse consequences while the plant was at power or during a transient in which the mitigating function of the system was not required, then these failure modes of electrical and mechanical components could be added to the PRA (if not already included in the models). Should there be no adverse consequences associated with inadvertent operation of these systems, then the spurious actuation failure mode of the digital system could be set aside.

By considering the digital system in context with the overall integrated plant design and focusing on the failure modes of the supported electrical/mechanical components, there may be significant potential for limiting the digital system failure modes of interest that should be included in the PRA and for which failure probabilities would be needed. Collaboration on the part of I&C personnel and PRA analysts to identify the overlap and differences between potential I&C related effects and the failure modes modeled in the PRA can facilitate a focusing of the scope of the digital system failure modes that may be useful to consider in the PRA.

Step 3: Identify potential digital CCF susceptibilities

In the first two steps, individual system and component failure modes of interest to the PRA that could be the result of digital system failures were identified. In this step, consideration is given to the potential that some digital system failures could have an effect across multiple systems and trains of equipment that are modeled in the PRA.

Common-cause failure (CCF) of hardware components within a digital system are treated in a manner similar to CCF within the mechanical and electrical systems of the PRA. That is, similar components subject to similar accident sequence conditions within a digital system may be subject to CCF. The guidance in this report suggests no changes in the modeling of hardware related CCF in this regard.

However, a difference in digital systems from their analog counterparts is the existence of software. CCF for software must be treated differently than traditionally performed for hardware. This is because software behaves deterministically rather than probabilistically and can have both inter- and intra-system common-cause effects.

In later steps of this process, methods for incorporating CCF into the PRA will be discussed. CCF can take several forms: intra-system CCF, inter-system CCF and CCF between I&C that can trigger initiating events and that which actuates or controls the mitigating systems. For the purpose of treating digital system CCF in PRA, it is suggested that the digital system initially be considered to be made up of three distinct parts

- Operating system
- Applications software
- Communications units

I&C personnel have an understanding regarding the design and operation of the operating systems, applications software and communications and can provide input as to the need for considering intersystem common-cause effects.

Step 4: Develop PRA model with simplified treatment of digital I&C

The purpose of this step in the digital I&C modeling process is to select or incorporate high level basic events or super-components that simulate I&C failure effects in the PRA that can be used in subsequent steps to evaluate the relative importance of the digital system. Reflecting the digital system in the PRA in this manner begins with incorporation of basic events in the PRA logic representing the digital system failure modes identified in Step 2 above that result in failure modes of the electrical/mechanical components modeled in the PRA that are actuated or controlled by the digital system. In addition, CCF related basic events should be included in the models where they were identified in Step 3.

Note from the first two steps that the plant systems and components into which the digital I&C logic is to be incorporated are already modeled in the PRA. As a result it may be possible simply to select existing basic events in the PRA to represent the functional effects of the digital I&C failure modes identified in Step 2. Alternately, the digital system behaviors initially may be represented using super-components incorporated into the PRA models at appropriate locations given the associated components and their failure modes identified in Steps 1 through 3.

Figure 4-1 provides an example showing the level of detail needed in the model for the purpose of supporting the sensitivity study of Section 5. The example illustrates where the effects of digital system failure should be considered in the PRA logic, including CCF effects.

Along with basic events representing the failure effects of the digital system, parameter estimation will need to be performed in order to incorporate digital systems into the PRA. In this regard, the PRA parameters representing digital systems may be:

- The probability of failure of the digital system actuating the required mitigating function for a given initiating event
- The beta-factors between the digital mitigating functions for the same initiating event both within a given digital system that supports multiple mitigating trains of equipment and across digital systems that support redundant mitigating functions and share similar software
- The frequencies of the failure modes of digital systems that lead to initiating events.

The actual values assigned to the basic events in the logic of the PRA representing digital failure are not particularly important at this stage. If the analysts wish to assign values that are representative of typical digital system failure probabilities, they may use any of the methods summarized in Section 5.1 of this guideline. What is important at this stage is to have basic events incorporated in the PRA, at least at a high level, which can be used to determine the importance of the various digital system failure modes. The sensitivity study described in the next step is used to identify which of the basic events representing digital system failures is important to the results and, therefore, worthwhile modeling in detail, and for which development of rigorous parameter estimates may be useful.

Step 5: Estimating the sensitivity of the results of the PRA to digital I&C failures.

Depending on the scope of digital systems in a given plant, a potentially significant amount of logic and parameter estimates may require development. However, not all of the systems, components or their parametric values are critical to the PRA: for a number of them, simplified modeling may be acceptable with assignment of numerical values that can be accepted relatively easily without significantly affecting the PRA result. Thus, the objective of the sensitivity analysis is to identify the digital systems and components that do and do not strongly influence the outcome of the application of the PRA. It is the digital systems and components to which the PRA results are sensitive for which more detailed logic and high reliability claims are necessary and simplified modeling and quantification methods may not be suitable.

A variety of approaches are available to establish whether or not the PRA is sensitive to a digital system and its failure modes. These approaches may involve:

- setting failure probabilities of digital system related events to artificially high values and then identifying any events that are dominating the results
- generating importance measures for the digital related events and selecting those that contribute significantly to risk now or could contribute significantly were they to be assigned a high failure probability
- qualitatively selecting digital related events based on knowledge of their design and functions in the roles that they play in managing the safety case.

Regardless of the method used to define digital system importance, the purpose of the sensitivity study performed in this step is to identify those digital systems to which the PRA and its application are or are not sensitive and categorize them as such. The sensitivity is determined by confirming that the results of the PRA (or its specific application) are not affected significantly when digital systems and their failure modes that are considered to be of limited importance to the PRA **collectively** are assigned relatively high failure probabilities (e.g., one to two orders of magnitude above that expected using the methods of Section 5.1). If the results of this sensitivity study suggest that the results of the PRA or its specific application are sensitive to selected digital systems categorized as being low in importance, or visa verse, then a recategorization can be performed.

On completion of the sensitivity study, the resulting categorization of digital systems as either having high or low sensitivity with respect to the decision being made should be presented to selected members of the plant staff for their consideration. In addition to I&C personnel, input from operations and engineering would provide valuable input as well.

Step 6: Incorporate I&C modeling detail into the PRA based on step 5 results

Two levels of digital system modeling detail are considered depending on the outcome of the sensitivity study performed in Step 5.

For those digital systems to which the decision being made is not sensitive, a relatively low level of detail is all that will be necessary, as the results of the analysis are not influenced significantly by this I&C. Models at the super-component level, similar to what may have been implemented for the sensitivity study in Step 5, may be all that is needed. The important aspects of these simplified, limited detail models is that shared resources between redundant mechanical and electrical trains of equipment and systems controlled by the digital systems be represented in the model (e.g., power supplies for the I&C, shared networks, etc.).

For those digital systems to which the PRA and decisions being made are sensitive, a greater level of detail in the modeling may be necessary. Figure 4-2 provides an example of a hypothetical system for which detailed modeling might be developed. For these systems, the I&C system can be broken into its various units and detailed fault trees developed as a function of these units. For example, a digital actuation system may include the following:

- Sensors
- Signal processing devices
- Communication units
- Voting logic
- Actuation devices

Note that the portions of the digital system under consideration for modeling in the PRA functionally are not unlike those typically modeled in PRAs for analog I&C systems. It is just that the component types would differ (e.g., devices with processors are being used for signal processing and voting logic as opposed to components such as voltage-to-pressure convertors and relays).

Additionally, each device containing processors will have associated software. In developing the PRA logic model, the software can be linked directly with the hardware in which its processors are installed, keeping in mind that where it is similar to software that is a part of redundant trains or systems, there may be both intra- and inter-system common cause effects that should be included in the logic. Note that the places that these CCF effects should be considered were investigated as a part of Step 3 above and remain the same for development of any new logic that is to be incorporated into the PRA.

Section 4 of this report expands further on methods for development of digital system logic models, both at the low level of detail when the PRA is insensitive to the system in question, and when greater detail is needed because the digital system may drive the results of the analysis.

Step 7: Estimate digital system/component failure probabilities

The next step is to develop parameter estimates (or failure probabilities) for the events incorporated in the PRA representing the failure of the digital system and its components. Like the level of detail in the modeling described in Step 6, the effort needed to estimate failure probabilities for the digital system and its components should be commensurate with the sensitivity of the results to the digital I&C in question. Approaches to parameter estimation in this report are developed in detail in Reference [9]. Section 5 in this report provides a summary of that reference.

For those digital systems for which it has been shown that the results of the PRA or specific application being performed are not sensitive, a ‘black-box’ approach is taken for which any number of state-of-the-art methods may be used to estimate the probability of failure at the system level. For example:

- Conformance with consensus standards that imply a potential reliability level
- Reliability growth methods

- Review of operating experience
- Fault injection methods
- Statistical testing.

Section 5.1 discusses a subset of these current state-of-the-art methods that are sufficient when high reliability claims are not critical.

A more rigorous approach is suggested for quantification of the reliability of digital systems and their components to which the PRA has been shown to be sensitive. This approach breaks the system up into its major parts (i.e., voting logic, signal processing, communication units, etc.) and examines the design in some detail with respect to defenses against important failure modes. Section 5.2 presents an approach for estimating failure rates for computing units within a digital system when detailed modeling and parameter estimation is in order. The approach uses a 'white-box' approach that may require examination of the details of the design of the computing units in the digital system. The approach addresses both the hardware and software that make up the digital system.

For hardware, the detailed modeling approach is similar to that which commonly is performed for analog systems only with different component types (e.g., signal processing units and voting logic as opposed to components such as E/P (voltage-to-pressure) convertors and relays). Where failure data may not be available at the computing unit level (again, signal processing units or voting logic), a review of the detailed design of representative computing units may be necessary in order to estimate a failure probability from vendor or generic data sources for subcomponents making up the computing units.

For software, the approach consists of four tasks:

- Development of a digital system reliability model

  The digital system reliability model developed in this task is a structured representation of the digital system developed only for the purpose of providing the numerical values for the events included in the detailed logic developed in Step 6. The digital system reliability model is not for the purpose of incorporating into the PRA logic. It focuses on the evaluation of design processes and digital system design features that address failure modes to which the PRA is sensitive. Following the development of this reliability model, available design and operating information will be used to derive the needed parameter estimates: development processes, system architecture, defensive measures, extent of tests and verification, operations and maintenance procedures, operating experience, etc.

  The digital system reliability model can be built starting from the hardware architecture of the digital system, where the system is decomposed into various units, such as instrumentation units (sensors and actuator controls), computing units (signal processing and voting logic), and communication units much in the same way the detailed logic is developed in the PRA in Step 6. Since the objective here is to estimate failure probabilities at the level of detailed modeled in the PRA, only parameter estimates at the digital unit level are expected to be needed, as opposed to data for modules or basic components within the computing units. The digital reliability model is then further refined by decomposing the units derived from the hardware architecture into smaller elements that either are or are not affected by the failure modes and mechanisms identified in Step 6 above.

The digital system reliability model also determines, for each digital system function to which the PRA is sensitive as identified in Step 5, the paths that are available internally to the digital system to perform the function. In this context a path identifies a set of elements of the digital system reliability model that together can perform the function. The model is then further refined by decomposing the units derived from the hardware architecture into smaller elements that either are or are not affected by the failure modes and mechanisms identified in the first task above.

As the architecture of the digital system may have features such as internal redundancy and internal functional diversity and separation, multiple paths could be available to perform the same digital system function. Thus, the digital system reliability model also includes representation of the potential for digital common-cause failures between its various elements, so that the potential for digital common-cause failure of the paths associated with a digital system function can be estimated.

Development of the digital system reliability model is an important task because it allows the analyst to take consideration and credit from a well-thought out digital system architecture. Beyond supporting derivation of numerical values for the PRA, it also can be used as a tool to help digital systems architects compare various options.

- Identification and classification of failure mechanisms

  In the first three steps of this section, failure modes of the digital system were identified and in Step 5, the sensitivity of the PRA to these failure modes was determined. A reliability model of the digital system was developed to the computing unit level for those systems to which the results of the PRA were sensitive. This task identifies and classifies the failure mechanisms within the computing units that could lead to failure modes determined by the sensitivity analysis to be significant to the PRA results. There is no single classification scheme applicable to all digital systems. A pragmatic approach is recommended, considering the known defensive measures that have been taken to prevent, eliminate or tolerate certain categories of failure modes or mechanisms.

- Assessment of Defensive Measures

  Measures are often taken during development or during system operation to minimize, or even eliminate, the occurrence of specific failure modes or failure mechanisms, including common-cause failure mechanisms. The objective of this step is to systematically identify these defensive measures, to associate them with the corresponding elements of the digital system reliability models built in the preceding tasks, and to assess their effectiveness with respect to the failure modes and mechanisms determined in the first task of this step.

This is an important step in the quantification of digital reliability, because it allows the analyst to take into consideration and to credit the effort made by the designers and the operators to limit the risks of failure and common-cause failure. It also allows the identification of weak points on which improvement efforts could be focused. Finally, it identifies the residual digital common-cause failure mechanisms that can still affect the system, and thus provides a linkage between the estimated beta-factor and its underlying basis in deterministic system behaviors.

The analyst applies engineering judgment to assess the coverage and effectiveness of the defensive measures and their impact on common-cause failures. Certain measures may be judged effective enough that the modes or mechanisms thus protected can be considered negligible with respect to other mechanisms (including non-digital mechanisms such as random hardware mechanisms or human errors). Others may be judged to be partially effective and not guarantee a complete elimination of the modes or mechanisms in question, but still reduce the potential for their occurrence or effects. Lastly, some modes or mechanisms may not be protected at all. It will be the objective of the final task of this step to estimate the effects of these residual modes and mechanisms on the occurrence rates of the critical failure modes.

- Quantification of Residual Failure Modes & Mechanisms

  The objective of this step is to quantify the occurrence rates of digital failure modes critical to the results of the PRA by considering the residual failure mechanisms (including common-cause failure mechanisms) that have not been ruled out by defensive measures.

  This step applies engineering judgment, considering the nature of the elements of the digital system reliability model that could be affected, and the weaknesses of the set of defensive measures. One can also use some of the state-of-the-art methods (Section 5.1), when their restriction to specific elements of the model or to specific failure mechanisms may help ensure that they are used within their validity limits.

Step 8: Regenerate the PRA results with final digital systems/components modeling

In this step, the logic models from Step 6 and parameter estimates from Step 7 are integrated into the PRA logic models. Basic events in the form of super-components or 'black box' logic are combined with estimates developed from current state-of-the-art methods such as those presented in Section 5.1 and detailed unit level logic with estimates developed using the more thorough 'white box' methodology described in Section 5.2.

In addition to accident sequence quantification, several sensitivity studies are performed. First, all of the digital systems to which the PRA was classified as not being sensitive are raised one to two orders of magnitude in failure probability collectively. The purpose of this sensitivity study is to confirm that the results of the PRA or the specific application being performed remain insensitive to these digital systems. Second, a review of the events added to the PRA logic is performed to identify those that are redundant in accomplishing the mitigating functions credited in the PRA. The purpose of this review is to identify those combinations of digital related events that are assumed to be independent in the analysis.

Step 9: Review/confirm PRA results, sensitivities, and insights

The final step in the incorporation of digital I&C logic into the PRA is to perform a review of the results and sensitivity studies. This review is best performed jointly by the I&C personnel and PRA analysts involved in earlier steps of the effort, as well as other members of the plant staff. The results of the specific application being evaluated using the PRA are discussed, along with key assumptions that influence the decision that is to be made. Conclusions should be explained in terms of plant design features and operating characteristics that drive the results.

The sensitivity studies are reviewed. A conclusion is drawn as to the validity of the classification of parts of the digital systems and components to which the results are not sensitive. Plant design features and operating conditions that make these systems low in significance are identified and confirmed. Assumptions regarding digital system and component independence are also reviewed. The defensive measures that result in redundant systems and components not having a significant potential for common cause failure are confirmed and noted for future reference in operating and maintaining the system.

Section 3: Concepts and Definitions

3.1 Concepts

3.1.1 Digital Systems and Equipment

In this document, term digital system is given a broad meaning, and includes all systems and equipment driven or controlled by software (running on microprocessors or microcontrollers) or by programmable electronic logic (running in application-specific integrated circuits (ASICs) or field programmable gate arrays (FPGAs)). In particular, this includes digital I&C systems, smart devices, and data communication equipment.

3.1.2 Digital Failure

The hardware portions of a digital system are subject to random failure as would be the case with analog I&C. Software, however, does not fail but behaves systematically (deterministically). Given the same inputs, it will produce the same outputs every time. It does not wear out nor is there anything random about it.

A digital failure requires two indispensable 'ingredients': a **digital fault**, and an **activating condition** (also called a **trigger**) for this fault. Without an activating condition, the digital fault would remain dormant and unrevealed. A digital common-cause failure requires these two ingredients, plus a third: the **concurrency** of the activating condition in multiple units of the hypothetical system. Concurrency here means that the activating condition occurs in the multiple units in such a short timeframe that corrective actions in the first failed unit cannot be performed before other units also fail. Figure 3-1 illustrates the relationship between faults, activating conditions and concurrency in their potential effect on software behavior in a digital system

For software to 'fail', therefore, it must contain a fault and encounter input conditions (a trigger) for which it was not designed and then respond in a manner that is detrimental to the system or component being able to perform its function (see Failure Mechanisms, Modes and Effects below).

In developing a probability of failure of a digital system and its software, we are estimating the potential for a fault combined with likelihood of the occurrence of the plant conditions or trigger for which the system was not designed and having it respond in a manner such that it does not perform its function.

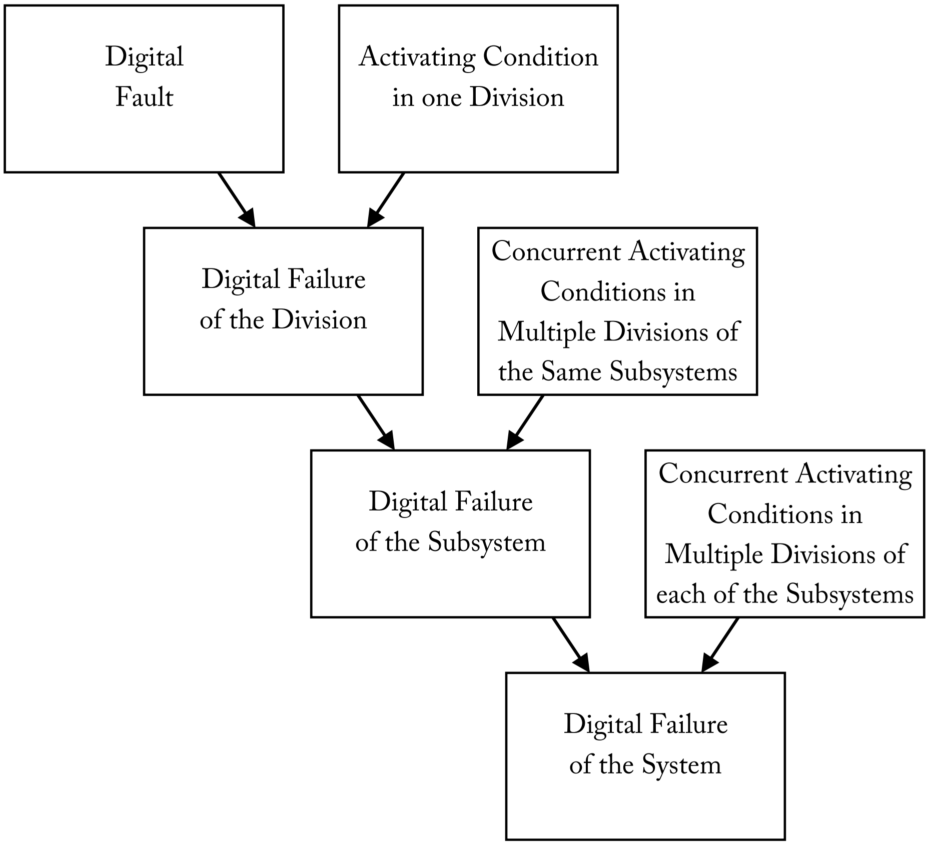

Digital Fault
Activating Condition in one Division
Digital Failure of the Division
Concurrent Activating Conditions in Multiple Divisions of the Same Subsystems
Digital Failure of the Subsystem
Concurrent Activating Conditions in Multiple Divisions of each of the Subsystems
Digital Failure of the System

Figure 3-1
The ingredients necessary to the digital failure of a hypothetical system.

3.1.3 Defensive Measures

Designed-in measures may be taken to eliminate or minimize the occurrence of particular failure mechanisms. Hereafter, such measures are called defensive measures (see [16]).

For example, freedom from divisions by zero may be guaranteed by different means, such as:

1. No division.
2. Formal verification using software static analysis tools.
3. Verification prior to each division, that the divisor is not zero.

Defensive measures may also be taken to eliminate or minimize the occurrence of particular failure modes.

In the case of a function providing a single Boolean result (e.g., 0 or 1) a no output condition may be prevented using a watchdog timer. The watchdog is set by the initialization of the digital system, and reset each time the system provides an output. If the system does not write its output on the output board in due time, the watchdog provides a default answer and raises an alarm signal to inform the operators.

Lastly, defensive measures may be taken to tolerate particular failure mechanisms and/or modes of the digital system so that they are not likely to cause unacceptable effects in the systems or functions controlled by the digital system.

For example, if a division by zero occurs, the system can be designed so that it will trigger a protective action (even when none is warranted), since a spurious actuation is considered acceptable, whereas a failure to actuate is not.

The inventory and analysis of the defensive measures, and the assessment of their coverage and efficiency, allow the identification of the residual failure modes and failure mechanisms, and also the identification of the dominant modes and mechanisms on which one should focus in order to quantify the reliability parameters necessary to the PRA.

3.1.4 Failure Mechanisms, Modes and Effects

While the systematic failure behaviors of digital systems may be characterized in terms of designed-in faults activated by specific triggering conditions (as described under Digital Failure), modeling digital failures in PRA requires an understanding of digital failures in terms of their mechanisms, modes and effects. These words have specific meanings in the development and quantification of PRA models. In general, failure modes and their effects are modeled in PRA. Failure mechanisms are not typically modeled in PRA, but are useful in the estimation of failure probabilities for digital system components (see Section 5.2). The following subsections offer clarifications and examples specific to digital systems, consistent to the definitions given in [10].

3.1.4.1 Failure Mechanisms

A *failure mechanism* is an event or chain of events occurring during operation and / or maintenance that can lead to the failure of a component, system or function. Failure mechanisms generally manifest themselves **internal** to the component or system. In mechanical components, examples include aging mechanisms, wear out, environmental degradation, etc. In PRA models, internal mechanisms may be causes of failure modes, but it is not common practice to model them explicitly.

Digital systems may be affected by *systematic failure mechanisms*. These differ from those of mechanical systems in that they are systematic with respect to operating conditions – a set of operating conditions that triggers a fault to cause a failure will cause the same failure every time those conditions occur. Randomness may affect the existence of the triggering conditions, but not the system behavior. This is different from hardware, in which small variations in wear out mechanisms introduce randomness in failure timing, even with identical operating conditions.

Postulated failure mechanisms are dependent on the design decisions made and on the implementation technology used. It is to be noted that different failure mechanisms may lead to the same failure mode of a given component, system or function.

For example, in a digital system, a division by zero may raise an exception resulting in a processor being stopped. The division by zero is just one of any number of mechanisms by which the processor may stop functioning, a memory protection violation or an error in the processors memory being examples of other mechanisms.

3.1.4.2 Failure Modes

A *failure mode* of a component, system or function is defined by the **external** behavior, as if the component, system or function is being viewed as a black-box. For digital systems, the postulated failure modes (i.e., the failure modes that are theoretically possible) are completely determined by the functional requirements applicable to, and the outputs of, the system, component or function. A priori, they are independent from the design and the implementation technology.

For a reactor protection function that has only one periodical Boolean output (decision to perform or not to perform the protective action, made at regular time intervals) locked when the protective action is triggered (output is latched in the triggered state), there are only three postulated failure modes:

1. Output of 1 instead of 0.
2. Output of 0 instead of 1.
3. No output in the required time frame.

This third failure mode may be subdivided into sub-modes, depending on how late the output occurs

As noted above, a given failure mode may be a result of one or more of any number of failure mechanisms. In turn, the failure mode of a component, system or function has an effect on the operation of the affected system or function. The external failure modes and effects of a system or component often are modeled explicitly in PRA logic models.

3.1.4.3 Failure Effects

A failure mode can be translated into its effects on the component, system or function in question.

For example, a mechanical valve failing to open would prevent flow through the piping train in the system in which the valve is located. Failure of flow through this piping train, in turn, has an effect on the function that the system performs (injection to the reactor, for example).

Using the reactor protection function in the example above, the effects of the postulated failure modes are:

1. Protective action when none is warranted.
2. No protective action when one is warranted.
3. Delayed protective action

Effects will depend on the design of elements external to the function. E.g., if the absence of output is detected by an external monitoring device, the device could trigger a protective action, whether it is warranted or not.

3.1.4.4 Failure Mechanisms, Modes and Effects Summary

Given the above, failure mechanisms of a component lead to failure modes of that component that then can have failure effects on the system in which the component resides. The component failure effects constitute failure modes at the system level. These system failure modes in turn have failure effects on the functions that the systems perform.

In PRA, the system level or functional effects typically are represented by the top events of the logic models (e.g., the headings of the event trees and tops of the fault trees – see discussion of PRA below). The component failure modes represent the lowest level of detail included in the fault trees used to quantify the event tree headings probabilistically.

In supporting the modeling of digital I&C in PRA, therefore, the failure modes and failure effects of systems (and possibly the components and their failure modes) often will be modeled explicitly. As a result, defining methods for quantification of digital system (and possibly component) failure modes is a focus of this report. Similar to the mechanical and electrical components included in PRAs, it is not necessary to determine failure probabilities for specific failure mechanisms of digital I&C to support accident sequence quantification. However, as will be seen in Section 5, a knowledge and understanding of digital related failure mechanisms and design measures taken to limit their potential or preclude them is very useful in estimating probabilities of the failure modes for digital components and systems that are included in PRA.

3.1.5 Probabilistic Risk Assessments (PRA)

The purpose of PRA is to evaluate the risks associated with an installation by modeling and analyzing the various accident or event scenarios that could lead to pre-defined unacceptable consequences. Classical PRA models are based on 'static' probabilistic event trees and fault trees.

Event trees are inductive logic models used to analyze initiating events that lead to a plant trip and operation of various mitigating systems. Event trees can be constructed to varying levels of detail, and can focus on either mitigating system or mitigating function success/failure. Fault trees are deductive logic models used to identify the combinations of components and their failure modes that would lead to the high level (top logic) unacceptable consequences defined by the event trees. Fault trees incorporate probabilities of the various failure modes so that their impact on overall risk may be assessed. The full set of event trees and fault trees for a PRA model offer a complete view of the plant relative to a given risk consequence. (For a nuclear power plant, this would typically be core damage frequency or frequency of release of radioactive products.)

This report describes methods for representing digital systems in the PRA and estimating the contribution of specification and design errors to the probability of failure of the I&C system functions, such that it can be incorporated into the event tree and/or fault tree logic models. The needed level of detail to which the I&C is modeled is left to the analyst, and will depend on the application of the PRA and the sensitivity of the results to the I&C modeling.

For some regulatory bodies, the main interest of PRA is qualitative, and they do not set targets for absolute values. Some regulatory bodies give a much higher significance to absolute values and require that the quantified values used in the models be thoroughly justified. The objective of this document is to help designers and PRA analysts in developing such justification for digital systems.

3.1.6 PRA Application

A specific application of a PRA is the evaluation of a particular issue based in part or whole on a plant-specific PRA and often documented in an analysis. Example applications of the PRA issues such as plant design changes, modifications to test or surveillance intervals, licensing amendments, evaluation of operating events or assessing the effects on risk of changes to day to day plant configuration for maintenance purposes in a nuclear power plant.

3.1.7 Parameter Estimation

Parameter estimation for use in PRA is the development of failure probabilities that are to be assigned to the basic events (components and their failure modes) included in the logic models of the PRA. In parameter estimation for digital systems, failure probabilities for both hardware components and any associated software will be needed.

Hardware components are subject to random failure and probabilities may be derived from a combination of generic data sources, vendor information or plant specific data. Development of random failure probabilities for hardware is a well understood process commonly practiced in PRA. Section 5.2.2 provides data sources from which digital system hardware failure probabilities may be derived.

Software is not subject to random failure but behaves systematically. In developing a failure probability for software, we are estimating the potential for there being a fault in the software along with the occurrence of a trigger that will activate the fault (as described earlier in this section under the definition of digital failure). Three types of software failures may require parameter estimates when modeling digital I&C in PRA:

- the failure probability of digital mitigating functions
- the frequency of spurious actuation of digital systems
- the potential (or beta factor) for digital common-cause failure.

The following provides further definition of each of these systematic digital system failures. Detailed description of methods for deriving parameter estimates for systematic failures is provided in Section 5.2.1 and Reference [9].

3.1.7.1 Digital Mitigating Functions

An example of a digital mitigating function for a digital system is assessment of plant process variables and the generation of commands within each of the divisions of a digital system in support of the initiation of automatic reactor trip signals and emergency core cooling (ECCS) signals. These digital systems support operation of other non-digital components within the mitigating system:

> Consider a safety injection system, as an example. The signal from the I&C only commands the injection valve to open; successful operation of the system also requires the motor, its power supply, and the valve itself to function properly.

Such functions can be decomposed into more elementary functions so that each elementary function is either completely performed by, or completely independent from, digital systems.

It is to be noted that a probability of failure on demand (or P_{df}) may be associated with each mitigating function of a digital system, the demand being made up of the plant conditions associated with a given transient or accident. It is also to be noted that multiple mitigating functions may be assigned to the same digital system, to address the same or different initiating events. From a digital failure standpoint, there is a priori no reason for different digital mitigating functions to have the same P_{df}, even when they are implemented by the same digital system.

> For example, function A may fail due to an incorrect or incomplete functional specification, and yield a functionally incorrect output. The digital system that implements function A is still operational even though A has failed. Another function B implemented by this system might still be able to perform correctly if it does not depend on A's incorrect algorithms or outputs.

Thus, one may speak of function failure rather than system failure. This remark leads to the conclusion that digital reliability is not applicable to the digital system itself: it can be estimated or evaluated for each of the functions assigned to the system. In a number of cases, in particular when a function has multiple postulated failure modes, it might be worthwhile to evaluate separately the occurrence rates of individual modes.

3.1.7.2 Spurious Actions of Digital Systems

Some initiating events included in the PRA, such as spurious reactor trip or spurious ECCS actuation, may be triggered by spurious or incorrect actions of particular digital systems. Thus, to correctly evaluate the full impact of digital systems in plant safety, one should identify these systems and the failure modes that can lead to initiating events, and estimate the frequency of these failure modes.

The explicit representation in PRA of these systems and spurious actions is particularly important if a possible common-cause failure between an initiating event and some of the digital mitigating functions for this event has a significant impact on PRA.

3.1.7.3 Digital Common-Cause Failure

One of the most valuable properties of well-designed and highly reliable digital systems is their deterministic behavior, which allows designers and analysts to predict how they will behave in all situations they may face. However, this strength is also at the origin of concern about digital systems, due to the fact that in case of specification or design error, deterministic behavior could lead to multiple and concurrent failures, or common-cause failures (CCF).

A number of approaches are generally recognized and accepted to protect against digital CCF, in particular defense-in-depth, separation and diversity. However, these approaches are not always fully applicable. For example, digital CCF could affect the redundant divisions of a reactor protection system, these divisions being in general identical or nearly identical in functionality and design. Digital CCF could also affect diversified functions implemented using the same I&C platform and components (hardware and software).

Often, PRA models represent CCF in the form of beta-factors, i.e., of the conditional probability of failure of one division of digital I&C given failure of another division. If the two divisions of I&C are identical, then the beta-factor can be high. That is, when two divisions in the same system are subject to the same plant conditions (e.g., identical inputs) and have the same functional specification and design, then when one division fails due to a software error the other division is likely to respond identically and also fail (i.e., a beta-factor of 1). As a result, intra-system common-cause factors for identical divisions performing the same function should be assumed to have a high beta-factor.

On the other hand, when different functions are performed by a digital system or the same function performed by different digital systems, the conditional failure of the second system or function may not be highly conditional on the first. In this situation, consideration should be given to developing a beta-factor that reflects the similarity and differences of the system designs that accomplish the system functions. While it is not routine to include inter-system common cause factors for hardware in PRA, similar software found in different mitigating systems can lead to the need for estimating a beta-factor.

Finally, it is to be noted that there is a priori no reason for beta-factors to be symmetric between digital systems or functions. As an example, similar digital systems implementing similar functions based on different plant conditions may have different beta-factors depending on the defensive measures used in their design and implementation.

3.2 Definitions

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

Activating condition. A specific condition affecting a digital system that activates and gives life to a dormant digital fault and causes a digital failure.

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].

Basic event. An event in a fault tree that requires no further development and generally represents failure of a component and its failure mode.

Beta-factor. The conditional probability of failure of redundant digital mitigating channels or divisions of digital I&C systems given failure of one division or channel of a digital I&C system (also referred to as common-cause beta-factor).

"Black box". System or component whose internal contents are not defined.

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. [IEEE 603-1998]

Common-cause failures. Concurrent failures (that is, failures which occur over a time interval during which it is not plausible that the failures would be corrected) 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.

Communicating station. Functional unit or device connected to a communication link, and that sends messages to, and / or receives messages from, the other stations connected to the link.

Communication link. Set of equipment and media that allow two or more communicating stations to exchange messages.

Components. Discrete items from which a system is assembled.

Computing unit. A ‘box’ within a digital system made up of components that collectively perform a given function in support of the successful operation of the digital system. Examples include signal acquisition and processing units, communication units and voting logic units.

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; the ESFAS supports the physical barriers to radiological release by cooling the fuel, actuating containment systems, and allowing time for other measures to be taken by reactor operators. [adapted from NUREG/CR-6303]

Design fault. Digital fault affecting the overall design of a digital system, its software or the programming of its FPGAs.

Digital fault. Functional requirement specification or design error resulting from the development of a digital system, and that exists in the system right from the beginning of operation.

Digital failure. A systematic failure resulting from the activation of a digital fault.

Digital Common-cause Failure (digital CCF). A systematic common-cause failure resulting from the activation of a digital fault.

Digital Mitigating Function. Portion of a mitigation function that is performed by a digital system.

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

Division. The designation applied to a given system or set of components that enables the establishment and maintenance of physical, electrical, and functional independence from other redundant sets of components. NOTE: A division can have one or more channels. [IEEE 603-1998]

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

Failure mechanism. An event or chain of events occurring during operation and / or maintenance, and leading to the failure of the system, component or function.

Failure mode. External behavior of a system, component or function in case of a failure, the system, component or function being viewed as a black-box.

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.

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

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.

Initiating event. An event either internal or external to a nuclear power plant that perturbs the steady state operation of the plant by challenge to control and safety systems. [ASME PRA Std.]

Intrinsic fault. Digital fault that can be recognized independently of the functional objective of the system, and without full knowledge or understanding of its functional requirements specification.

Oracle. Any program, process, or body of data that specifies the expected outcome of a set of tests as applied to a tested object. [NUREG/CR-6848]

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

Parameter. In this report, a numerical value in a PRA that represents a P_{df}, a beta-factor or a frequency of spurious operation associated with a digital system.

Partial failure. Failure of a component or a subsystem that does not prevent the whole system from performing an expected or required function.

Random fault. Fault appearing at a random time, which results from one or more of the possible degradation mechanisms in the hardware

Random fault or failure. Failure, occurring at a random time, which results from the activation of one or more random faults

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. [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]

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. [3]

Specification fault. Fault in the functional requirements specification of a system.

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).

Train. An arrangement of components that make up a single path of a mechanical or electrical system (non-I&C).

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

Section 4: Detailed Guidance on Modeling Digital I&C in PRA

This section provides detailed guidance supporting Steps 4 and 6 of the process described in Section 2. It discusses modeling digital I&C in PRA at two different levels of detail. The initial modeling of digital I&C (Step 4 in Section 2) is for the purpose of estimating the sensitivity of the results of the PRA to digital I&C failures. The results of the sensitivity studies performed with this high level modeling (Step 5 in Section 2) is used as input to determining the level of detail needed in PRA logic for the various digital I&C systems and the rigor needed to develop failure probabilities for the digital related events (Steps 6 and 7 in Section 2). On determining the sensitivity of the PRA or its applications to the digital systems being incorporated in the PRA, some systems could be sufficiently important that they may be selected for detailed modeling. On the other hand, the PRA and the specific applications being evaluated with the PRA may be insensitive to many digital I&C system failure modes. When this is the case, significant detail and justification for high reliability claims may be unnecessary. The following sections provide guidance on modeling of digital I&C for the initial sensitivity study (Steps 4 and 5 of Section 2) as well as for incorporating the final level of detail required in the modeling (Step 6 in Section 2).

4.1 Scope of Digital I&C in PRA

I&C systems play a variety of roles in support of nuclear power plant operation and response to transient and accidents. Digital systems can be of benefit in many of these roles. As the PRA primarily is concerned with plant response to transient and accident conditions, this section discusses roles that digital I&C may play on the potential for or response to a transient or accident and the influence of those roles on determining the level of modeling detail that would be useful to consider in the PRA.

4.1.1 Normal Plant Control Systems

Detailed modeling of normal (non-safety-related) plant control systems in the PRA generally should not be necessary. Success for these systems is more often a function of plant response and performance, rather than a function of either hardware or software reliability (e.g., whether the feedwater pumps are turbine or motor driven, how much of an overcooling, pressure or level transient occurs during the initial stages of the event, operating procedure guidance, etc.). This is true of both analog and digital control systems. For example, consider the control of a main feedwater (MFW) pump following a reactor trip. Some plants automatically bypass the normal three element control of feedwater flow in preference to a predetermined flow setpoint or switch to single element control. In addition, it is not unusual for a swell in steam generator or reactor level to cause a high level trip of the feedwater pumps following a plant trip. Beyond that, all plants have EOPs that instruct the operator to take manual control of the feedwater system if it remains available. Given typical plant conditions following a reactor trip, what drives the probability of success of a normally operating control systems is plant response to the transient (e.g., fluctuations in steam generator or reactor level, the power transient resulting from changes in primary and secondary coolant temperatures, EOPs, etc.), not I&C system reliability.

In the PRA, the failure of these systems at power is generally included in the initiating event frequency. For these systems, the important failure mode of the I&C is reflected at the system functional level, regardless of how the digital system itself may fail. Digital I&C system technology is expected to contribute to reduction of initiating event frequencies, because these systems are more responsive and can contain algorithms that can be more finely tuned than analog controls. This will likely be proven in time (already there is experience to this effect in both US and European plants that rely upon digital balance of plant controls). A PRA that relies upon traditional initiating event frequencies, with a plan to update the frequencies when plant-specific data are available, will be bounding.

The normal plant control systems generally provide pre-initiating event functions and are not of much interest to the PRA post-trip. A few normal plant controls (such as for MFW) may be given limited post-trip credit in some PRAs; however this credit is rarely extensive, and never solely relied upon. A minimum amount of fault tree modeling of initiating events may be necessary to capture dependencies (e.g., shared components or support systems), and the purpose of these models is to ensure that credit is not given post-trip for a system or component that was involved in the initiating event.

Another issue to consider is whether there are any unique or complex initiators that can be caused by a credible failure of an integrated digital control system (Step 2 in Section 2). For PRA, this issue is no different than for an analog integrated control system, except that it is easier to design such a system with digital controls (because computers may perform multiple functions). Hence the PRA should consider whether there are credible integrated control system failures that can cause conditional failures that are not considered within one of the traditional initiating events already included in the PRA. A failure modes and effects analysis (FMEA), such as is typically performed by the design activity, is a good tool for making this determination. A typical result of an FMEA, for example, would be the incorporation of design defenses against spurious control system actions through the distribution of critical control functions amongst different computers.

4.1.2 Mitigating System(s)

In developing a PRA, a number of mitigating systems are called upon post initiator to assure the three main safety functions are maintained (primary coolant system integrity, reactor shutdown with adequate core cooling and the prevention of significant releases). The mitigating systems that provide these functions can be a mix of safety-related and non safety-related. Dependencies between these mitigating systems considered in the PRA include not only shared equipment but, where digital systems are used, common software between redundant systems.

The plant protection system, consisting or reactor trip (RTS) and actuation of engineered safety features (ESFAS), should be a primary I&C focus for the PRA. Since the protection system is a multi-function entity with varying degrees of redundancy and diversity, it is important that the PRA capture the dependencies and potential CCF contributions while simultaneously crediting the design features of redundancy and diversity that (per industry consensus design standards and practices) provide reliable and robust performance.

Non safety-related mitigating systems also are considered in the PRA, generally for accident sequences that go beyond design basis events. These may include diverse systems required by regulation (e.g., ATWS systems) or balance of plant systems that are capable of backing up the functions provided by the safety systems (e.g., main feedwater, fire system, containment venting, etc.). Whether these systems are controlled by digital I&C may vary from plant to plant. Where these systems share dependencies with initiating systems or other mitigating systems, these dependencies are generally developed in the PRA (Step 4 in Section 2).

For mitigating system digital I&C, it is important to capture the failure modes that may lead to the loss of the mitigating system function. The failure modes of individual components within the mitigating system itself dictate the level of detail needed in modeling the I&C. A bounding analysis may assume that the digital failure modes are such that the mitigating system components fail in the least convenient direction. Where such failure modes are excluded, an engineering rationale should be developed providing justification for their exclusion.

4.1.3 Supporting Control Systems

Once the plant protection system performs its function to actuate safety-related systems, there may be a few closed loop control systems required to maintain the operation of the mitigating systems. This may include system-specific controls such as component cooling water control or steam generator level control. Where these are safety-related controls, they are independent of the non safety-related normal plant control systems. These are generally simple linear or proportional controls, with little or no integration needed between functions. The consequence of failure is easily modeled as a failure mode of the final controlled device(s) (which may be conservatively assumed to fail in the least convenient direction, if desired). However, like the protection system and other mitigating control systems, these separate control functions may share common hardware, software, or support systems and the dependencies should be resolved in the PRA (Step 4 in Section 2).

4.1.4 Main Control Room Instrumentation Systems

Main control room (MCR) instrumentation systems are typically not modeled explicitly in the PRA. Adequate instrumentation is assessed in the human reliability analysis (HRA). This includes implicit modeling of instrumentation dependencies in the HRA if there are dependencies upon the initiating event (e.g., power dependency). The diversity and redundancy of instrumentation is usually sufficient that its failure is an insignificant contributor to the HRA, and its reliability can be included in the HRA, if this is not the case. Symptom-based EOPs[11]often provide appropriate guidance irrespective of the availability of specific instrumentation, further reducing the significance of modeling operator informational I&C in the performance of human reliability analysis.

Non safety-related controls and displays in the control room are designed so that a credible failure will not interfere with automatic protection system functions. Conversely, the manual control systems credited for diversity and defense-in-depth (D3) assessments are independent of the postulated protection system computer failure.

For these reasons, it is not necessary to include detailed modeling of main control room instrumentation in the PRA.

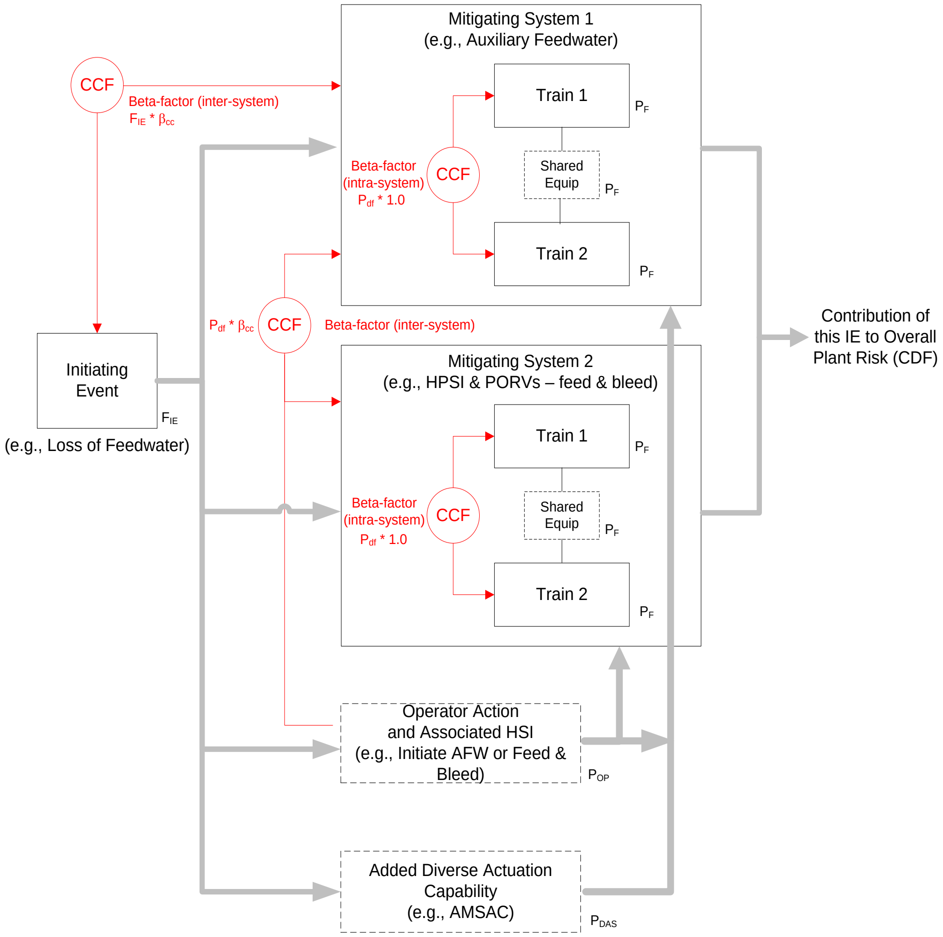
4.2 Level of Detail of PRA Model for Mitigating System Digital I&C

The digital system related parameters introduced above are further illustrated in Figure 4-1, which highlights the relationship between them and the mechanical and electrical systems and equipment that the digital systems actuate and control. In Step 5 of Section 2, an evaluation of the sensitivity of the PRA to the various digital system functions was suggested. Figure 4-1 illustrates the level of detail useful in performing this sensitivity analysis. The final level of detail to which a given digital system needs to be modeled in PRA (Step 6 in Section 2) depends on the application of the PRA that is under consideration and the sensitivity of the decision to be made on the digital system and its reliability.

In Figure 4-1, events within the front line mitigating systems, between the front line mitigating systems, and as potential causes of initiating events are used to represent the effects of failure of the digital system. Where digital systems are used to actuate supporting systems, such as service water or ac power, super-components representing the digital system should be added at high levels in these systems as well.

Whether developing high level or detailed digital I&C models, it is important to include dependencies between redundant systems and divisions whether shared resources or common-cause effects. Dependencies on shared resources, such as power supplies, can be incorporated in the logic consistent with traditional PRA methods in which systems or components in the model are logically linked with supporting systems.

Digital common-cause effects, which can have both inter- and intra-system impacts (see Step 3 of Section 2), can be added as super-components as illustrated in Figure 4-1. If in Step 3, it was concluded that CCF was not likely, for example between systems using different plant parameters for actuation and functionally diverse actuation, then a basic event representing that CCF need not be added to the logic models. For the purpose of determining the need to incorporate CCF susceptibilities in the PRA logic, the following general guidance is proposed.



Notes:
1) P_{df} = channel failure probability (Factor A)
2) Beta-factors reflect the CCF potential (Factor B)
3) The four mitigating systems and redundant trains show the existing D3 (Factor C)

Figure 4-1
Digital I&C Relationship to Mitigating Systems Modeled in the PRA

Operating system common-cause

For a plant wide digital system, the operating system can be common to many plant systems, both mitigating systems as well as normal operating systems. It is expected that high quality digital systems that perform critical functions in support of plant operation will have operating systems that are designed to perform cyclically, with few interrupts and are not affected by plant conditions. As an initial determination of whether common-cause failure of the operating system should be modeled explicitly, those operating systems that do not exhibit these three characteristics should be considered to be potential sources of CCF across associated plant operating and mitigating systems.

Applications common-cause

Traditional practice in the design of I&C for mitigating systems is to reduce the potential for CCF by use of functional and signal diversity. This practice is common whether considering analog or digital systems. Review of operating experience confirms the importance of functional and signal diversity in addressing the potential for CCF [7, 8]. The presence or absence of functional and signal diversity in a digital system design is suggested as an initial determination of whether CCF of applications software should be considered in the PRA. This functional and signal diversity should be reviewed not only within mitigating systems but across mitigating systems as well.

Communications unit common-cause

Similar to the operating system, cyclic operation with transmittal of information that is transparent to the values communicated results in limited potential for the communications units to contribute to failure of the digital system. Communications units that do not have these two characteristics are candidates for consideration of CCF between divisions of a system and across mitigating systems.

In cases where the PRA or its specific application are shown to be insensitive to the digital system in question, the level of detail illustrated in Figure 4-1 is sufficient. That is, fault trees representing digital I&C at the digital system level is appropriate with an emphasis on incorporating shared dependencies and common cause failure modes. Common cause modeling not only should include intra-system I&C effects but intra-system as well, as identified by I&C specialists in Step 3 of Section 2.

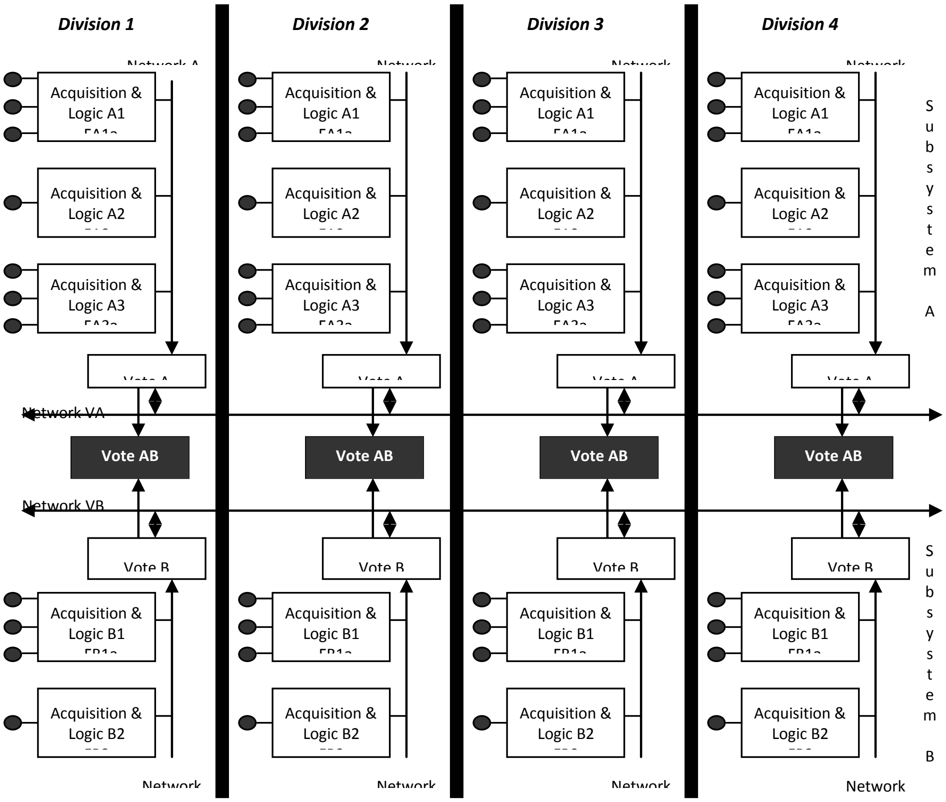


Figure 4-2
Architecture of Hypothetical Digital System

Where the results of the PRA or its application are sensitive to the manner in which the I&C is modeled, a greater level of detail is necessary. Figure 4-2 illustrates a hypothetical digital protection system. It consists of five functionally interdependent computing units or component types:

- Sensors
- Data acquisition and processing units
- Communication networks
- Voting logic units
- Actuation devices

When detailed modeling of the digital system is useful in making decisions based on the results of the PRA, fault tree logic representing each of these component types or computing units and their failure modes are appropriate. This more detailed fault tree logic would be developed to replace the high level I&C logic shown in Figure 4-1 (the I&C represented by the CCF of the digital systems within and between the mitigating systems). Note that this level of detail is not unlike that which may already exist for important analog I&C protection systems that are modeled in the PRA. The principal differences would be that the component types for data acquisition/processing and voting units would differ (e.g., devices with processors are being used as opposed to components such as signal converters and relays).

The software and hardware are coupled, and should be treated together. Since the software resides on the hardware (i.e., the computer processor), it does not exist outside of the computer. Therefore the digital system hardware (with appropriate CCF factors) provides a good surrogate for PRA modeling of the software. The processor may exist at the signal processing, communications or logic level within the digital system. Alternately the functional effects of the software failure can be represented at the component, division or system level. The approach is to link the software CCF probability to the hardware upon which it resides. Digital system or component failure probabilities are discussed in Section 5 and depend on design processes, design features and defensive measures employed by the designer to address potential failure modes and mechanisms associated with the digital system. The CCF probabilities (also discussed in Section 5) will consider the case of hardware that shares common software, whether it be common operating system (OS) or application software. In this respect, software failure can be treated as a failure mode of the hardware.

4.2.1 Physical and Functional Considerations

The level of detail of the PRA model should be appropriate to resolve physical and functional dependencies. Since the computers may perform multiple functions, a level of detail at the system unit level reflecting these functions is appropriate to resolve these dependencies (e.g., sensor, signal processor, voting, etc.) However, a higher level of detail, such as subsystem or train, may be appropriate if failure rate data is available or can be estimated at that level. For example, if multiple, redundant ESFAS functions are on the same system, then a level of detail that shows the shared equipment (e.g., common unit, common subsystem or common division) will bound the effect of the shared hardware and/or software, given the incorporation of appropriate CCF events in the models (considering both intra and inter-system effects).

The chosen level of detail also needs to address the effects of the functional or other diversity not only within the I&C but the plant systems in which the I&C resides. Here again, the digital system unit level of detail, or higher, is appropriate, assuming that the diverse functions are distributed to different units, subsystems, or divisions. If all of the functions rely upon the same unit, subsystem, or division are assumed to fail simultaneously, then the results will be bounding, and can demonstrate the benefit of any diversity that exists. This assumes that there are applicable CCF factors between the redundant units, subsystems, or divisions to account for identical software. Here again, the context of the digital system within the plant as a whole is important in determining the level of detail required in the I&C modeling. Where digital I&C controls multiple redundant mitigating systems, consideration of any diverse means of actuating these systems in the model will reduce the importance of the digital I&C. Where it controls only a single mitigating system, less detail is acceptable.

In general, going below the unit level of detail is neither advised nor practical. Failure of the digital system unit should be considered an all-or-none proposition. This will provide a bounding result with regard to the software contribution. However, modeling below the digital system unit level of detail, and modeling failure of individual failure mechanisms independently is problematic, if even possible. That approach requires excessive detail, may not be supported by available data sources and creates an extra burden relating to quantification of software and hardware reliability that may not be important given the context of the digital system with respect to the integrated plant design as well as existing deterministic defense-in-depth and diversity design features.

4.2.2 Other Hardware Aspects of Digital I&C Systems

Many aspects of I&C system design for safety related applications will be fail-safe. For example, outputs may be de-energize-to-trip, energize-to-trip, or analog (such as for a closed-loop control). The PRA should consider the potential failure modes of a unit, division or system's digital output (fails on, fails off, fails as-is). Certain failure modes can be eliminated from consideration if not credible or not applicable to the modeled consequence. For the failure probability of a digital I&C system units, it is the analyst’s choice whether to parse out the failure probability by failure mode, or take a bounding “all-modes” approach. However, parsing of the failure probability into failure modes may require a more detailed evaluation of a unit's internals or its operational history (see Section 5.2).

Another question is how to treat fault-tolerant designs. Fault-tolerance is the built-in capability of the system to continue correct execution in the presence of a limited number of hardware or software faults. Self-testing and fault-tolerant features are prevalent in digital I&C system designs. “Coverage” is an important concept, as it determines the percentage of failures that are self-monitored (i.e., self-revealing) versus non-self-monitored (or test-revealed). This failure mode breakdown will vary between I&C designs and between different types of digital components. It has an important role in the PRA analysis, as it drives which mathematical unavailability model (repair-time model, test-interval model, or both) is used for each component.

Certain failure modes are easily detected by the fault-tolerant circuits. For example, this includes failure of fiber optics. Not only are fiber optics useful for isolating the propagation of energy-related faults, their failure is easily recognized by the fault-tolerant design. Since fiber optics carry an “active” signal, “cutting” the fiber link results in an instantly recognizable fault, which can never be interpreted as a valid input.

Fault-tolerant design can be treated explicitly in the model, or it can treated conservatively to reduce modeling complexity. For example, consider a four-channel system with 2-of-4 redundancy. The corresponding fault tree logic for this would typically consist of failure of 3-of-4 channels. However, for a fault tolerant design, this may not result in system failure. For a covered fault of one of the inputs, the typical fault-tolerant program would inhibit the faulted input and adjust the redundancy to 2-of-3. An additional covered fault might reduce the redundancy to 1-of-2, or result in defaulting to the safe state (per designer preference). Beyond this, LCOs will generally limit the time the plant is allowed to operate in this configuration. Hence, for covered faults, the failure logic in the fault tree may be more accurately portrayed as 4-of-4. It is relatively straight forward (albeit tedious) to model the dual logic in the fault tree, representing the failure logic as 4-of-4 for covered failure modes and 3-of-4 for non-covered (or mixed) failure modes. However, in the interest of reducing modeling complexity, and at the cost of some additional conservatism, it is often preferred to model all of the failure logic the same (3-of-4 in the example). This is usually not a huge conservatism, because the failure probability of the system is typically dominated by the non-covered faults, and by CCF.

4.2.3 Test and Maintenance Considerations

A final consideration in the development of digital I&C logic for use in PRA is test and maintenance effects. The preceding steps in this section address the hardware and software aspects of the digital I&C systems being modeled. The influence of testing and maintenance unavailablities or potential errors that might be made that affect the reliability of the digital system subsequent to these activities have not been included up to this point (nor are they necessarily addressed in the parameter estimation methods of Section 5).

Unavailability due to testing or maintenance of digital systems can be treated in a manner similar to that which may be currently performed for analog systems. When super-components are used to represent the digital system (as may be the case when the results of the PRA are insensitive to the I&C), it may be appropriate to consider test and maintenance activities a part of the 'black-box' estimate that makes up the failure probability for the super-component. This is particularly true if it can be shown expected test and maintenance events are staggered, that is they do not occur simultaneously. However, when more detailed modeling is considered to be necessary, when a division of I&C is removed from service occasionally, then an estimate of the amount of time it is out of service can be made and converted to an unavailability that can be incorporated into the I&C logic as an event by itself. The need for such an event can be determined based on the response of the system to removal of specific digital system components from service. For example, if the out of service component results in the placing of the division to a state in which it is providing its function or if the unavailability of the component results in the system converting to a more conservative state (e.g., 2 out of 3 vs 2 out of 4 for actuation), then there may be no need for including these maintenance unavailabilities in the model. Similarly, periodic testing that does not disable the automatic functions of a digital system provides justification for not adding such activities to the logic.

The more interesting impact of maintenance and testing activities is assessing the potential for introducing errors in the system that may render it incapable of performing its intended functions. In addition to errors in functional specifications for digital systems (see Section 5.2.1.3), errors resulting from test and maintenance have been shown to contribute to operating experience [7, 27].

Events representing test and maintenance errors are already included routinely in existing PRA models (i.e., pre-initiator human errors such as fail to restore from service, miscalibration, etc.). Methods for estimating these pre-initiator human error rates are well developed [29, 30], involve review of maintenance and testing procedures and can be used to estimate the probability of errors common to analog and digital systems as well as extended to include estimates of digital system related errors in the PRA (e.g., updating incorrect software or data sets).

For a digital I&C system with a high level of redundancy and diversity, a potentially conservative model might demonstrate that the risk is not sensitive to the digital I&C reliability or the level of modeling detail. A PRA that models the functional effects of digital failures (at the mitigating system or train level) is capturing the risk relevant design characteristics of the system.

Section 5: Parameter Estimation in Digital Systems

The purpose of this section is to define practical options for developing values for digital system parameters (i.e., failure probabilities) for use in PRA. It provides detailed guidance to support Step 7 of the process described in Section 2. Methods described in this section in large part are based on the specifics of the digital systems that are the most important to the safety of nuclear power plants. These systems are usually developed specifically to the requirements of the nuclear industry, and have relatively similar design and operating principles. In addition, their licensing usually requires a detailed knowledge of their development process, of their design, of their behavior and of their operating and maintenance procedures. Thus, the significant amount of information available regarding the design of these systems may be used as inputs to the proposed quantification method.

As noted in the introduction, there is no claim that parameter estimation methods for digital systems or components are precise. Indeed, it is not sure that high accuracy is possible, even in theory. It relies as far as reasonably possible on objective facts and aims at minimizing the part of subjective human judgment. While there is uncertainty associated with the methods, they achieve the objective of estimating a given parameter within orders of magnitude ranges that can be justified, as this is considered sufficient for use in PRA.

For digital systems to which the PRA and its applications are not sensitive, the digital failure rates used in PRA are generally easier to justify and current state-of-the-art methods are sufficient. These state-of-the-art methods are summarized in Section 5.1.

For digital systems that play a more significant role in the PRA and decisions being made in its application, a more detailed approach is proposed. This approach examines the design of the digital system and the presence or absence of defensive measures that address potential failure modes and mechanisms of units within the system. This more detailed approach is presented in Section 5.2.

The methods for parameter estimation proposed in this section are discussed in detail in Reference [9]. The following sections largely are a summary of that report. For more detail on the concepts and limitations of these approaches, Reference [9] should be consulted.

5.1 Parameter Estimation (Black Box Analytic Methods)

The methods presented in this section are intended for use when the claimed failure rates (P_{df} or frequency of spurious actions) are not too ‘ambitious.’ None of these methods for quantifying digital systems reliability is universally applied or accepted, in particular for highly reliable systems. Therefore, the suggested methods essentially provide rough estimates for digital system failure rates and must be supplemented using engineering judgment.

The black box methods illustrated in this section support development of failure rates at a level of detail shown in Figure 4-1, that is at the digital system level rather than for individual units or components that make up the digital system. The sensitivity study performed in Step 5 of Section 2 demonstrated that the results of the PRA or its application are not sensitive to selected digital systems. A coarse level of detail and use of black box methods to approximate digital system failure rates having this characteristic are sufficient.

In developing rough parameter estimates for digital systems for use in PRA, the estimation of digital system failure rates will be discussed first followed by common-cause factors that may be applicable both within and between systems.

5.1.1 Estimating Failure Rates (P_{df})

Reference [9] describes a number of state-of-the-art black box methods, including the principles and limitations associated with each method. For practical purposes, two of the methods described in that reference are the most likely candidates for use in estimating digital system failure rates in PRA using black box methods: interpretation of operating experience and demonstrating conformance with consensus standards. A third approach, statistical testing also may be possible, although the practicality of this approach and resources needed to implement it given the limited significance of the systems in question may be impractical. Again, these approaches must be supplemented with engineering judgment regarding the design of the digital systems in question. Therefore, I&C specialists having knowledge of the digital systems being represented in the PRA are required.

5.1.1.1 Operating Experience

Unique applications of digital systems may not have a great amount of operating history on which to draw. Therefore, if operating experience is to be used, it may be necessary not only to consider that from the nuclear industry, but other industries as well. Statistical evidence on the operational experience of comparable digital systems is a 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 significant operational experience without a single report of a potentially unsafe digital failure.[2] 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 1. 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 100 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 (on the order of 5E-6/demand).

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 that may lead to the same consequences (which is also estimated based on the vendor records).

[2] An order of magnitude estimate can be derived by assuming that there are in the range of 10 000 commercial aircraft with digital controls (mostly Airbuses and Boeings), with an average of 5 years in operation that fly roughly 8 hours a day. This yields more than 10,000 operating hours without an unsafe digital failure.

Note. 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 2 Probability of Digital Failure With Limited Information.

An alternative device to the trip unit of Example 1 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}/demand. Whether the PRA shows that using this failure probability the trip unit may become a significant contributor to risk for some events will depend on the context of the unit with respect to the overall plant design.

For additional assurance beyond operating experience, defensive measures such as those listed in Tables A-1 and A-2 of Appendix A 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 3. Impact of Defensive Measures in a PLC Platform.

A PLC platform is being used as part of an ESFAS upgrade. 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. In addition, a review of the design is performed that provides additional assurance of high quality by looking beyond the primarily process-based assessment documented in the SER. Selected behaviors and defensive measures are confirmed by review of documentation and/or testing. 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, which is not as low as for a system with significant operating experience (see Example 1) but is better than a system which only has been confirmed to meet current standards (see Example 4).

5.1.1.2 Comparison to Standards

Use of appropriate hardware and software development standards is one factor in assuring digital system reliability. IEC 61226 [12] 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 [13] addresses software, while IEC 60987 [14] addresses hardware.) This risk figure applies to the whole of the system from sensors to actuation devices and is intended to encompass all sources of failure due to specification, design, manufacturing, installation operating consideration and maintenance practices. The standard consists largely of software development process requirements and the suggested failure probability should be considered to be the best that can be expected on the basis of process alone. To justify a lower failure probability estimate, defensive measures beyond just process would need to be present, such as those in Tables A-1 and A-2. Indeed, a number of regulatory agencies[3] 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 A-1.

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

The PLC platform from Example 3 is being used as part of an ESFAS upgrade. Again, 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 Appendix B 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

[3] In France and in the UK (with justification supported by statistical testing and formal verification).

concluded, for the purposes of 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 5. 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 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 (i.e., under its Appendix B 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.

Estimates such as these are comparable to the safety integrity level four (SIL-4) risk targets from IEC standard 61508[15]. Application software development processes used in SR nuclear power plant I&C systems are generally comparable to or better than SIL-4, which suggests that a limit to the application software failure probability of 10^{-4} to 10^{-5} is a reasonable value.

Table 5-1
IEC 61508 – Failure Rates According to Safety Integrity Level (SIL) [15]

SIL	Low demand mode (Probability of failure on demand)	High demand mode or Continuous mode (Probability of a failure per year)
4	≥ 10–5 to < 10–4	
3	≥ 10–4 to < 10–3	
2	≥ 10–3 to < 10–2	
1	≥ 10–2 to < 10–1	

5.1.1.3 Estimation of Common Cause Factors (β_{cc})

It should be noted that while the methods of Reference [9] may be used to approximate the reliability of selected digital systems, none of these methods provide an indication regarding digital common-cause failure rates, even for moderately reliable systems. Therefore, in this section, guidance is provided with respect to developing common cause beta factors that may be appropriate to consider. Both intra-system and inter-system effects are discussed.

General experience with rigorously designed and highly reliable digital systems shows that the predominant causes of digital failures are usually functional specification faults [17, 27, 7]. A change in plant conditions that activates a functional specification fault and causes a digital failure may also cause 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.

An equally important consideration is that of inter-system effect for platforms having varying types and degrees of diversity.

Example 6. Different Platforms Implementing the Same Functional Specification for the Same Mitigation Function.

The PLC from Example 3 is 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 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 are functional mistakes. Consequently, the intra-system beta-factor representing the digital CCF of the two channels is assigned a value of near 1. Thus, the use of diverse manufacturers, equipment and software has a limited effect on the failure probability of the system as they are not addressing the dominant cause of possible system failure.

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 A-1), there is a reasonable assurance that the likelihood of inter-system digital CCF is at least an order of magnitude less than the digital failure probability .

Example 7. Like Platforms in Systems Implementing Similar Functions Activated in Different Plant Conditions.

The PLC platform from Example 3 is to be used in two different systems. One system implements safety injection recirculation on low refueling water storage tank level. The other implements automatic auxiliary feedwater actuation on low steam generator water level. The algorithms and (analog) sensors share some similarity. 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 Table A-1).
- Because of the protection coverage of the defensive measures, it is estimated that the most likely cause of digital failure are functional mistakes.

Because the plant conditions 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 systematic, and the beta-factor can be assigned a range of values (10^{-1} to 10^{-3}) based on the degree of dissimilarity of functions and defensive measures.

Example 8. Like Platforms in Systems Implementing Very Different Functions.

The PLC platform of Example 3 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 Table A-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, and the beta-factor is negligible for the purposes of the PRA (see Tables A-1 & A-2).

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

Example 9. Beta-Factor for Simple Device.

The engineering evaluation of the trip unit of Example 5 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., much less than the likelihood of common mode failures due to maintenance or calibration errors), and that the beta-factor is negligible for the purpose of the PRA.

5.2 Parameter Estimation (White Box Analytic Methods)

In contrast with the state of the art methods mentioned in Section 5.1, the method proposed here is based on a 'white box' approach. That is, it takes advantage of all the available information regarding the system. In most cases this should not be a major obstacle: if high reliability rates must be claimed (and justified) for the PRA to give acceptable results, this usually (but not necessarily) means that the corresponding functions rank high in the safety classification. The licensing of the systems that implement them may require detailed knowledge of their development process, of their architecture, of their design and of their functioning.

This white box analytical approach requires a deep understanding of the digital system and is often more difficult to apply than the holistic methods of Section 5.1. However, it is in most cases an indispensable ingredient of a realistic reliability assessment: it allows the analyst to consider and credit the actual designed-in behaviors of the system as determined and constrained by the internal architecture (contrary, for example, to the quantification methods based on conformance to IEC 61508, which, for software, focuses mainly on the development process). It also allows the analyst to consider and credit the defensive measures taken by the designers or the operators to avoid, eliminate or tolerate certain types of failure modes and failure mechanisms.

The proposed method may make use, for specific issues, of some of the current state of the art methods, such as operating experience or statistical testing (see Section 5.2.1.4 regarding quantification of residual failure modes and mechanisms). It does so making sure (as far as reasonably possible) that they are used within their applicability domain and that the issues mentioned in the corresponding Limits paragraphs of Reference [9] are avoided or resolved.

As noted in Section 4, digital system hardware and software are coupled. The software does not exist outside of the hardware (processor) and therefore they can be modeled together. When detailed modeling of a digital system is desirable, however, parameter estimation at the digital system component or unit will be needed. At this level of detail, methods of parameter estimation for hardware and software differ. In this section, an approach to development of parameter estimates for software is discussed followed by references for sources of data for hardware. Once again consideration is given both to the context of the digital system in the plant design as a whole as well as to defensive measures that have been employed in its design, development and installation.

5.2.1 Parameter Estimation (Software)

In the second step of Section 2, the failure modes of interest for the digital system were identified. These digital system failure modes were based on the functions provided by the mechanical and electrical systems and the specific failure modes of the components making up those mechanical and electrical systems.

Example components and their failure modes that are modeled in a PRA would be ECCS valves failing to open or breakers to injection pumps failing to close. The digital system failure modes of interest would include those that result in no actuation signal or no output.

A four step process is suggested for digital system software parameter estimation. This process is implemented best by I&C specialists having familiarity with the design of the digital system.

1. Development of a digital system reliability model
2. Identification and classification of failure mechanisms
3. Assessment of Defensive Measures
4. Quantification of Residual Failure Modes & Mechanisms

5.2.1.1 Digital System Reliability Model

The failure modes of the digital system were developed based on the failure modes of the plant mechanical and electrical equipment that are actuated and controlled by the digital system (see Step 2 of Section 2). A relatively detailed model of the digital system was then developed down to the units that make up the digital system (see Figure 4-2 of Section 4.2). An early step in the software parameter estimation process is to develop a simple reliability model of the units that make up the digital system (e.g., data acquisition units and voting logic which contain processors). As noted in Section 2, this reliability model is separate from the PRA and represents only the digital system units. It is not intended that details would be placed in the PRA.

As examples, the software modules within the acquisition and logic units, the inter-division voting units, and the data communication units can be described as presented by Figure 5.2. Each computing unit (acquisition and logic, or inter-division voting) supports one or several application functions, each function being defined by a functional specification and implemented by a piece of application-specific software. This application-specific software may make use of one or several standard elementary functions provided by the I&C platform. Finally, each computing unit is driven by an operating system in charge of initialization, inputs-outputs, self-testing, communication with other units and computers (for example engineering or maintenance workstations).

For a given digital system, the operating system likely is the same for all computing units. The standard elementary functions may also be the same, but different application functions may use different standard elementary functions, each in a specific manner.

One or more communication units are associated with each computing unit. The communication units likely contain identical network system software, with network-specific and application-specific configurations that specify the communications between the computing units of the network (which computing units are part of, and allowed to connect to, the network, what information a computing unit can send to the network, and to whom, etc.). The communication units of a given network also may have identical configurations.

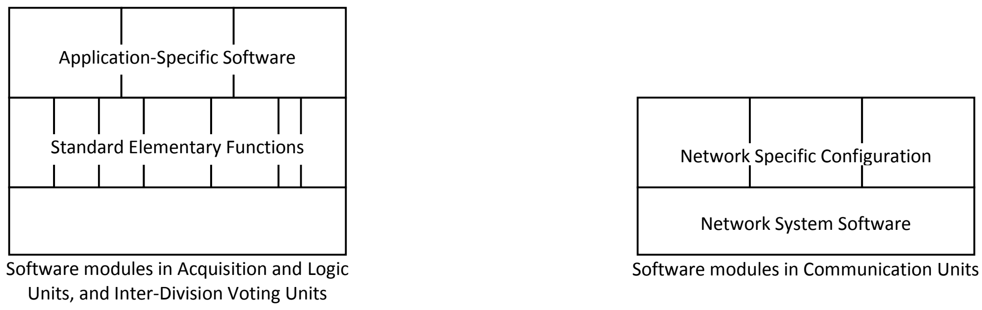

Application-Specific Software
Standard Elementary Functions
Software modules in Acquisition and Logic Units, and Inter-Division Voting Units
Network Specific Configuration
Network System Software
Software modules in Communication Units

Figure 5-1
Details of the digital system for which failure mechanisms are defined.

Finally, the reliability model identifies, for each of the digital system functions and failure modes determined in the first three steps of Section 2, the corresponding paths and the elements of the model the failure of which could result in one of these failure modes.

5.2.1.2 Identification and Classification of Failure Mechanisms

As a next step in estimating failure rates of software for components (units) within a digital system, the previously identified failure modes of the software are broken down into possible failure mechanisms that may lead to those failure modes. As is practiced in development of nuclear power plant PRAs, the level of detail in the logic models themselves will stop at the failure modes and will not include failure mechanisms. The potential failure mechanisms are being examined for use as input to estimating the failure rates. For a given digital system, the following classification of failure mechanisms might be applicable:

- design errors in the operating system of the computing units of the I&C platform.
- errors or inadequacies of the functional specification of an application function.
- design errors in the specific logic (software or logic design of an FPGA) of an application function.
- design errors in one of the standard elementary functions of the I&C platform.
- errors in the application-specific configuration of one of the data communication networks.
- errors in the system software of the communication units of the I&C platform.

As has been noted previously, the classification of digital failure mechanisms is mainly guided by the defensive measures that can be claimed. Defensive measures directed at addressing the above failure mechanisms are discussed in the next section.

5.2.1.3 Assessment of Defensive Measures

In this section, a review of the design of the computing units of a digital system is described for the purpose of assessing whether defensive measures are in place that address potential failure mechanisms that may be associated with tbe various computing units. The objective of this review is to screen failure mechanisms (and associated failure modes that have been addressed by defensive measures and identify the residual failure mechanisms (and failure modes) that dominate the potential for failure of the computing units. It is these dominant failure mechanisms on which the analyst would focus to develop failure probabilities for the computing units.

As introduced in Section 3, defensive measures are those design features and process elements used by the designer and owner to eliminate, reduce the potential for or tolerate failure mechanisms and/or modes of digital systems that may lead to undesirable effects in the systems or functions that are controlled by the digital systems. Each of the sub-elements of the units that make up the digital system are examined to identify existing defensive measures that are incorporated into the design or design processes for the purpose of addressing failure mechanisms that were identified in Section 5.2.1.2.

A rigorous discussion of defensive measures and their ability to limit the potential for digital failures, including common-cause, is found in references [9 and 16]. These reports not only describe specific defensive measures, but provide a detailed discussion of the basis for their effectiveness in addressing failure mechanisms and modes that could occur in digital systems. The following is a summary that relies to a significant degree on Reference [9]. For a more rigorous discussion of the types of defensive measures commonly used in the design, manufacture and operation of digital systems, References [9 and 16] should be consulted,

In the following subsections, a discussion is provided regarding defensive measures that are effective in addressing failure mechanisms in operating systems, standard elementary functions, application software, functional specifications of applications, communications units and common cause failures. The objective of reviewing potential failure mechanisms against existing defensive measures is to identify residual failure mechanisms (and their associated failure modes) that may dominate the probability of failure of the computing units of a digital system. Development of failure probabilities for the computing units given the dominant failure mechanisms is discussed in Section 5.2.1.4.

Defensive Measures for the Operating System of the Computing Units

The same operating system may be present and active in all the computing units (both the acquisition and logic units and the inter-division voting units) of a given digital system. It could thus be a significant agent of digital common-cause failure.

As introduced in Section 3, certain conditions must exist for a digital failure or CCF to occur:

- A digital failure requires two indispensable 'ingredients': a **digital fault** (in this case a design error in the operating system), and an **activating condition** for this fault. Without an activating condition, the digital fault would remain dormant and unrevealed.
- A digital common-cause failure requires these two ingredients, plus a third: the **concurrency** of the activating condition in multiple units of the hypothetical system. Concurrency here means that the activating condition occurs in the multiple units in such a short timeframe that corrective actions in the first failed unit cannot be performed before other units also fail.

Given, the above, a number of defensive measures can be taken and implemented in the operating system of a hypothetical system to avoid these conditions. These are mainly:

- A periodical, cyclic behavior where, after an initialization phase that is performed only once, the computing unit repeats at each cycle the same sequence of actions with as few variations as possible.
- The transparency of the operating system with respect to plant and reactor conditions and to the applications. In other words, the operating system actions do not change during plant transients or accidents.
- The diversity of the operation and maintenance conditions of the various divisions and subsystems that use the operating system.

In addition, Table A-2 provides further design measures that are commonly used in limiting the potential for digital failures in critical digital systems.

Defensive measures such as these, along with the formal verification of their correct implementation, can be used to allow the analyst to conclude that the operating system is not likely to be a dominant source of system or subsystem failure or common-cause failure.

Standard Elementary Functions

Standard elementary functions (also called function block modules) are an integral part of the I&C platform system software, like the operating system of the computing units or the system software of the communication units. As such, they could be suspected of being at the origin of digital common-cause failures.

However, these functions often have very favorable features: they are in general small, simple, independent from one another, without internal state variables, and rely on proven algorithms. Thus, they can, and have been verified individually (including with formal methods) to an extremely high level of confidence in their freedom from residual design fault.

For a well-designed system, one can conclude that, like for the operating system of the computing units and the system software of the communication units, the standard elementary functions are not likely a dominant source of digital failure and digital common-cause failure within the hypothetical system. Newly implemented functions may not have as much evidence to support such claims, but where such concern exists, the user may choose not to use the suspect modules.

Application-Specific Software

The application-specific software in critical digital systems often is developed according to a semi-automatic process, where the diagrams of the functional specification are manually translated into lower level diagrams expressed in terms of the standard elementary functions of the I&C platform. These lower level diagrams may then be translated automatically into executable binary code.

This process leaves a number of opportunities for errors: possible errors in the manual translation, and also possible errors due to the imperfection of automatic translation tools. However, besides the normal verification and validation process (including independent V&V), a number of additional defensive measures can be applied, such as:

- The formal verification that the intermediate C code complies with the specification of the application functions.
- The formal verification that the executable binary code is consistent and equivalent to the intermediate C code.

- Like the operating systems, the application-specific software has a periodic, cyclic behavior. Its influence factors other than those related to the reactor process are kept to a strict minimum.

It is possible to assure that faults in the application-specific software are unlikely to be dominant. In addition, for protection against CCF, they benefit from the functional diversity of applications.

Functional Specification of Application Functions

A number of measures are common during the development of digital systems to minimize the potential for errors in the specification of the application functions, such as those provided in Table A-1.

For purely Boolean application functions, such as the inter-division voting functions, fault avoidance and verification measures such as these, including test coverage, may be rigorous enough to provide adequate assurance that the specifications (and the application-specific software) are error free. One may be able to conclude that the specification errors affecting the inter-division voting functions are not likely to be a dominant source of digital failure and digital common-cause failure.

However, for acquisition and logic functions, it is in general very difficult to reach the same level of confidence, particularly for the more complex ones. This is mostly due to the fact that functional specifications are at the very beginning of the application development process, and there is no absolute reference on which a rigorous verification can be based. This conclusion is confirmed by the analysis of the operating experience of real digital systems; a number of cases have been identified where the functional specification has not been fully appropriate (for example, see [17]). Therefore, one must conclude that specification errors affecting the acquisition and logic functions cannot be excluded a priori, and that a specific quantification effort should be performed for these failure mechanisms.

A positive aspect for the functional specification of acquisition and logic functions is that functional diversity can provide a good defense against CCF: an error affecting an application is likely to affect only that application.

Communication Units

The system software of the communicating units can be designed following the same principles as the operating system of the computing units:

- Cyclic, periodic functioning with as few influence factors as possible.
- Transparency with respect to reactor process and application functions.
- Diverse operating and maintenance conditions in different divisions and subsystems.

Cyclic, periodic functioning can be ensured by the fact that within each network, at each cycle, the same set of messages are transmitted, in the same order, each message having always the same length, from the same emitters to the same receivers. Messages are transmitted even in the absence of their emitters or their receivers. Thus, each network has a constant load whatever the conditions. Only the values transported by the messages may vary from one cycle to the next. In addition, the configurations of the various networks of a digital system are often generated automatically, based on the low level diagrams of the application functions. They also may benefit from the periodic, cyclic behavior of the network and of the drastic minimization of the influence factors.

Like the operating system and the standard elementary functions of the computing units, communication unit software and the networks configurations with appropriate defensive measures should not be a dominant source of digital failure and digital common-cause failure for a hypothetical system.

Common-cause Failures

Regardless of what mechanisms may dominate digital failures, consideration also should be given to the potential for common-cause failure (CCF) and an examination of defensive measures to preclude them. Several sources of common-cause failure are considered.

CCF due to Concurrent Activation of the Same Errors

Functional specification errors may affect the acquisition and logic functions, which could lead to common-cause failure of individual functions across divisions. Because software behaves systematically, this means identical functions responding to the same conditions are likely to have a very high potential for common-cause failure. For this reason, identical software with the same inputs should be considered for assignment of a high beta factor (near 1.0).

However, functional diversity and separation between subsystems and between the acquisition and logic units of a division can be provided such that common-cause failure should not affect the other acquisition and logic units not implementing the failed function. The inter-division voting units should not be affected either.

If a CCF is due to an inadequate functional specification, the failure of an acquisition and logic function could even leave other functions performed by the same acquisition and logic unit unaffected, if these functions do not depend functionally on the failed function.

CCF Due to Failure Propagation

Various defensive measures can be implemented to reduce the potential for common-cause failure due to failure propagation within a digital system, e.g.,

- Restrictions on data communication.
- Stable and constant-load data communications.
- Plausibility checks (so-called ‘data validation’)

- Limited interface between computing units and communication units, through double-entry registers.

Again, References [9 and 16] provide greater detail regarding the effectiveness of these defensive measures.

With sufficient measures such as these, one may conclude that failure propagation through data communication links is well-protected. The only remaining CCF mechanism would then be the propagation of incorrect but plausible data, mainly towards the inter-division voting units.

CCF due to Shared Stress Conditions

The main principle in the defense against shared stress conditions is to avoid such conditions as much as reasonably possible. As has been seen previously, examples of defensive measures include:

- Particular dates and times cannot affect the hypothetical system, since dates and times of the day are not managed by, and are unknown to, the system.
- Overloading of the system, of its computing units and of its networks is prevented by stable, periodic, cyclic functioning.
- Operator requests are performed only one division and one subsystem at a time. There is indeed a stress condition, but it is not shared by the other divisions and the other subsystems.
- Demand conditions set by the reactor process affect all divisions and both sub-systems. However, they do not affect the most widely shared elements of the reliability model such as the operating system of the computing units.

Again, with sufficient defensive measures, one may conclude that adequate protection against common-cause failure due to shared stress conditions has been provided.

5.2.1.4 Parameter Estimation for Residual Failure Modes and Mechanisms

The conclusion of the preceding section is that while many potential mechanisms for digital failure can be reduced in their probability through application of appropriate defensive measures, a number of digital failure mechanisms cannot be guaranteed to be excluded for highly reliable digital systems and may need further complementary studies in order to quantify their occurrence rates. These are notably the failures of the acquisition and logic functions, mostly due to possible specification errors, and to a lesser extent, due to possible design errors.

The analyses also show that digital common-cause failure mechanisms can be well protected against, suggesting that the use of a single I&C platform for multiple subsystems and their various computing units, and the extensive use of data communication networks, do not mandate the use of beta-factors of 1.

The following paragraphs discuss possible approaches to estimate the P_{df} of individual acquisition and logic functions followed by a discussion of the estimation of probabilities of digital common-cause failures.

Estimation of Probability of Systematic Failure of Computing Units

Two principle approaches for estimating failure rates for software in the computing units of digital systems are proposed; analysis of operating experience and statistical testing.

Analysis of Operating Experience

If operating experience is to be used, it may be necessary not only to consider that from the nuclear industry, but other industries as well. Statistical evidence on the operational experience of comparable computing units in non-nuclear applications is a factor that may provide indication of bounding or practical estimates of digital failure probabilities for use in estimating computing unit failure rates in PRA. This would require access to this data or possibly obtaining it directly from the vendor. Absent such vendor information, operating experience reported for the nuclear industry may still provide a relatively significant basis for parameter estimation, even though somewhat limited.

Studies on the operating experience in the nuclear industries of digital systems important to safety have been performed in several countries (in particular in the US [7] and Korea [18]) covering a large number of systems and long periods of time. The data is consistent with the assertions of Section 5.2.1.3 Assessment of Defensive Measures in that digital faults have not been dominant contributors to actual or potential failures in safety-related digital systems.

Quantitative estimates of digital system units based on actual operating experience have been published as well [19, 20].

By definition, operating experience refers to systems already installed and in service. Considering the high reliability claims that need to be made for safety systems, operating experience must refer to systems that have been in operation for a long time period, and if possible, in a large number. The above references provide a collection of operating experience that begins to meet these characteristics and can be used in its current form to provide parameter estimates for use in PRA.

There are two principle sources of operating experience data that typically are available for existing nuclear plants, surveillance testing and actual demands in response to operating events. The most extensive source of data is likely to be surveillance testing. However, there are limitations to using testing data as the primary input for estimating digital component reliability with respect to systematic failures (i.e., software related). Software does not fail randomly; the measure of its reliability is the probability of it encountering conditions for which it was not designed and responding in a manner that is adverse to safety. Because testing procedures are generally similar each time they are performed, they are not likely to uncover unusual conditions under which software failures might occur. Therefore, while testing and operating demands may be adequate for evaluating the reliability of the hardware that makes up the digital system, only the operating demands are legitimate in assessing the reliability of the software.

Further review of the operating experience reported in the preceding references may be worthwhile, the actual operating demands in particular, to determine not only the types of failures encountered and their causes, but the operating time frame (or number of demands) over which they occurred. If the amount of time over which this operating experience occurred is significant, then it may be sufficient to approximate failure rates from this information. References [9 and 18] attempt just this, 1) reporting and interpreting the actual operating experience from digital safety systems installed in operating nuclear plants, and 2) estimating the operating time (or actual demands) and proposing quantitative methods for deriving failure rates at the digital system unit level. The digital protection systems investigated in these two references were designed, manufactured and are operated consistent with many of the defensive measures described in Section 5.2.1.3. Because of the extensive use of defensive measures, the most likely sources of digital unit systematic failure for these systems were judged to be functional specification errors affecting the application software or, to a limited extent, design errors. From the above references, the number of demands and failures of computing units in the installed plant protection systems over the time period under review was known.

- Over 500 reactor operating years of experience was available
- Approximately one actual demand on the plant protection system was estimated per reactor operating year.
- There are roughly 50 computing units per plant protection system of which 20% are assumed to be challenged during a given demand.
- Experience for the plants in the above references indicates that there were no systematic digital computing unit failures during any demand.

The approach taken in estimating the failure rate from operating experience for computing units within a digital system is one that is commonly used in PRA. The method to estimate the reliability of a system or component considers actual experience based on the operating time (or demands) and number of failures observed within the system. For this case, Jeffrey's non-informative prior [21] is used, because no systematic failures of the computing units have been experienced in the plant protection systems of the two references. The probability of failure on demand (P) of a computing unit is estimated using the following relationship.

$$P = (n + ½) / (d + 1) \qquad \textit{Equation 5-1}$$

where:

n is the number of failures that have been observed and

d is the number of demands.

n = 0 failures

d = 500 reactor years * 1 demand/ operating year * 50 * 0.2 computing unit demands/protection system demand

P = (0 + ½ failures) / (5000 computing unit demands)

= 1E-4 / demand.

The above failure rate may be a reasonable estimate for computing units in digital protection systems for which defensive measures such as those discussed in Section 5.2.1.3 have been implemented in the design for the purpose of limiting systematic failure of the operating systems, communications unit, elementary functions and application software. To use this failure rate on other protection systems, the effectiveness of defensive measures for those systems would need to be demonstrated by identifying relevant failure mechanisms using a white box approach to review computing unit designs. Even when such defensive measures have been implemented, computing unit designs cannot be guaranteed to be free of faults. However, the failure causes would be expected to be dominated by functional specification faults and unidentified design errors. As these are the expected dominant contributors to systematic failure of computing units for the plant protection systems investigated in References [9 and 18], then it is reasonable to expect other that other nuclear plant protection systems would have similar characteristics and failure rates.

Statistical Testing

From the discussion in Section 5.2.1.3 – Assessment of Defensive Measures, the main suspects leading to digital failures for a well designed system are the application-specific parts of the acquisition and logic functions, mainly due to their specification, but also, to a lesser extent, to errors made in the software development process.

In this context, and for typical plant protection system functions, well-designed statistical testing could be performed. If selected, several limitations identified in Reference [9] would need to be addressed.

- Uncertainties regarding demands statistical profile. This issue can be simplified if the main focus can be limited to application functions, the inputs and state variables of which are systematically identified. Specific verification can be performed to guarantee that any assumptions on inputs and state variables do reflect reality.

- Test conditions not necessarily representative of real conditions. It should be verified that application functions have a very short memory, and that a few seconds or a few minutes are sufficient to put them in conditions they would meet in real operation.
- CCF between the hypothetical system and the oracle. This sensitive and difficult issue can be resolved by the oracle using a diverse approach from the system.

One can derive the P_{df} value for the acquisition and logic functions critical to the PRA based on the number of statistical tests successfully performed.

Estimation of Common-Cause Factors

As noted earlier, defensive measures can be implemented to protect against digital common-cause failure mechanisms to assure that the system is well protected and that the use of the same platform hardware and software throughout the system does not systematically mandate the use of beta-factors of 1 between units. Common-cause methods were discussed in Section 5.1 (black box methods). While those methods considered the development of digital system common-cause modeling at a super-component level, the concepts are similar at the computing unit level. That is, four general conditions are of interest when estimating common-cause factors for systematic failures:

- Implementation of the same functional specification for the same mitigating function.

  Because of the deterministic behavior of software, identical software with the same inputs will respond in an identical manner on receipt of those inputs. This implies that a systematic failure of a computing unit, say a data acquisition/signal processing unit, in one of four divisions of a digital system is highly likely to occur in all four identical computing units of that digital system. This suggests a beta factor of 1 between the four identical computing units. Should the failure be a result of the functional specification, perhaps due to unanticipated plant conditions, the erroneous or incomplete specification would have an effect on all four divisions, and the high beta factor would apply regardless of whether redundant computing units were supplied by different manufacturers.
- Implementation of similar functions under different plant conditions.

  An example of this condition might be one system implementing safety injection recirculation on low refueling water storage tank level, and a like system implementing automatic auxiliary feedwater actuation on low steam generator water level. The algorithms and (analog) sensors share some similarity. But the similarity ends there, because these are different functions, actuating different components under different plant conditions in different time frames. Consideration of some common-cause effects between computing units is in order, but not with a beta factor near 1. The similarity in function, inputs and algorithms may put the beta factor on the order of 0.1 to 0.001 depending on the degree of dissimilarity of functions and defensive measures.

- Implementation of very different functions.

  An example of very dissimilar functions might be actuation of ac power sources (diesel generators) on bus under-voltage and initiation of safety injection on low pressurizer pressure. As long as defensive measures have been taken against technical AND functional mistakes that could cause digital CCFs (see Table A-1), the common-cause beta factor can be assumed to be negligible.

- Simple devices.

  Simple devices, easily tested, backed by a strong development process, a design that uses appropriate defensive measures, and an operating history that is both extensive and successful, should have a potential for concurrent failures in multiple channels that is relatively low (e.g., much less than the likelihood of common mode failures due to maintenance or calibration errors or common-cause failure of the hardware). [31] The beta-factor for systematic failure is negligible for the purpose of the PRA.

5.2.2 Parameter Estimation – Hardware

As is the case for any system modeled in the PRA, the parameter estimates for the hardware in a digital system will be dictated by the component failure modes that have been incorporated in the fault tree logic which, in turn, need only be developed to the level of detail required to support the decision being made using the PRA for a given application. In practice, the availability or absence of data sources often dictates the level of detail used in the logic models.

For the purpose of identifying data sources for digital system hardware that is associated with a digital system to which the results of the PRA are sensitive, the hypothetical system of Figure 4-2 is considered. This figure considers five different component types (sensors, data acquisition and processing units, communications networks, voting units and actuation devices).

A few of these component types are typical of I&C systems, whether analog or digital: sensors and actuation devices, for example. For component types and their failure modes that are commonly modeled in PRAs, the usual sources of data are all that may be needed for the purpose of developing hardware failure rates (see Reference [22], for example). Generic failure rates can be updated with plant-specific sources of information where operating experience is available and convenient to implement. Common-cause failure rates also can be developed in a manner consistent with current practices using information such as that published in Reference [23].

Other component types in the hypothetical system are not commonly modeled in current PRAs, as mitigating systems at existing nuclear plants may only make limited use of digital systems, at least in the United States at this time. These component types would include the digital data acquisition and processing units, communications units and the voting logic. Generic data sources for such component types are not readily available. However, the basic hardware components making up these units are known and it is proposed that from published data for these basic components, and with knowledge of the context of the units and how the units are designed, estimates of the failure probabilities of the units can be developed.

As is the case with software associated with an important digital system, a white box approach is proposed in reviewing the design of the hardware for the computing units in the digital system. An initial step in this approach is to examine what basic components make up each of these computing units. Figure 5-2 provides an illustration of what may make up data acquisition/ processing and voting logic units. In this illustration, it can be seen that the units consist of several modules (I/O, CPU, networks, etc.) that communicate through a backplane.

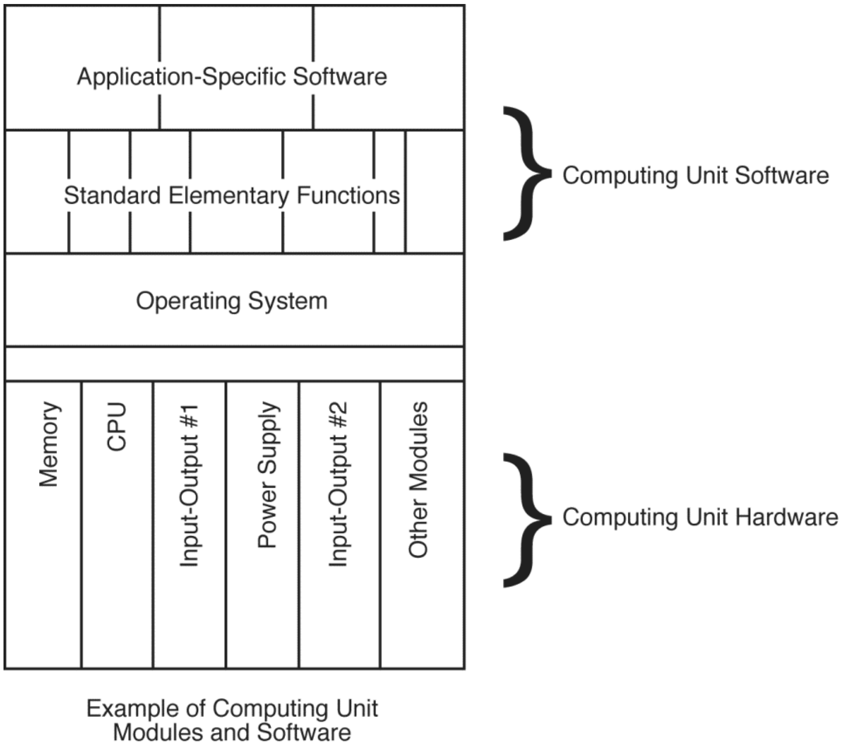


Figure 5-2
Modules from which computing unit parameter estimation is performed.

It is not suggested that the model detail in the PRA itself be expanded down to the digital hardware module level or its basic components. Rather, a simple model representing a typical computing unit can be developed, failure probabilities assigned and then an overall failure probability for the unit in question derived for the purpose of assignment to all similar units in the fault trees. This approach is essentially the same as that taken in Section 5.2.1 for estimating software failure rates and consists of reviewing the design of the computing units, identifying the basic component failure modes that contribute to the inability of the digital system to perform its functions, considering failure mechanisms that may lead to these failure modes and mechanisms and crediting defensive measures which may exist to limit the potential or consequences of these failure modes and mechanisms. In developing the simplified logic model for the computing unit hardware, credit for defensive measures such as redundancy, fault tolerance, whether or not failures would be monitored and announced or would be latent until a subsequent test or demand, as well as the designed-in response of a computing unit to a failure (e.g., fail safe, in a master slave configuration or monitored by components such as a watchdog timer). The model developed for computing unit parameter estimation could be in the form of a fault tree or a simple reliability equation. The overall failure probability for a computing unit could be estimated as described above and assigned to all similar computing units in the digital system.

As noted in Section 5.1, sources of data for computing units, modules or basic components that make up the digital equipment could be obtained from the vendor and may include information from operating experience of similar components in both the nuclear and other industries (such as chemical or aviation). If data from the vendor is not easy to obtain, several generic data sources could be considered. Among them are databases such as the Military Handbook [24] , EPRD-97 and NPRD-2011 [25, 26], which contain estimates of failure rates for digital related hardware such as microprocessors, integrated circuit components, memory modules, circuit boards, gate arrays, etc. A number of review and critiques of these sources of data for use in PRA have been published [27, 28]. These reviews provide comments on both the scope and limitations of these and other databases.

Common-cause failure of the hardware also should be considered, Common-cause factors could be developed in a manner similar to that currently used for mechanical and electrical equipment already modeled in the PRA. Data sources such as Reference [23] are appropriate. While digital components are not explicitly listed in that data source, recommendations are made with respect to CCF of generic hardware components that would be applicable.

Section 6: Summary

The purpose of this report is to provide general guidance on modeling of digital I&C in nuclear power plant PRAs. In developing this guidance, emphasis has not been placed on assuring precision in the modeling or parameter estimation as it is not expected to be necessary for most applications of the PRA nor is it practical. Rather, the guidance in this report focuses on recognizing the context of the I&C within the overall plant design, in particular with respect to failure modes of the electrical and mechanical equipment that it actuates and controls, as well as accounting for common design practices and processes implemented by designers and owners that are intended to ensure the reliability of critical digital systems in the form of defensive measures.

Consideration has been given in the guidance to determine the level of detail needed with respect to logic model development as well as parameter estimation. Consistent with industry practice and regulatory guidance, the necessary level of detail should depend on the application of the PRA and how sensitive the results and decision being made are to assumptions regarding the design and reliability of the digital systems. Sensitivity studies are suggested as the principal means of determining the necessary level of detail with high level (black box) methods being adequate when the results are not sensitive to the digital systems. More detailed (white box) methods are appropriate when the PRA is sensitive to details of the digital I&C system design and its failure rates. When more detailed modeling and parameter estimation is determined to be of value, modeling to the component type or computing unit level is suggested (e.g., sensors, data acquisition and processing, communications, voting logic and actuation devices) as opposed to developing logic down into basic components (e.g., circuit boards, processors, etc.).

Also consistent with current practice, modeling of digital systems considers the failure modes of the digital system and its computing units (e.g., failure to initiate a signal, spurious operation, etc.) rather than attempting to model failure mechanisms (e.g., task crash, corrupted output, specification error). However, failure mechanisms may play an important role in the estimation of failure rates and the manner in which the design addresses them using defensive measures. Characteristics of digital systems that are well designed with respect to such failure mechanisms are identified in the guidance in the form of defensive measures that address such mechanisms.

Guidance on parameter estimation considers the design of the system and identifies several available methods including comparison with consensus standards, statistical testing and taking advantage of published operating experience.

Finally, the guidance emphasizes that the development, quantification and application of digital system models in the PRA is a joint effort between I&C specialists familiar with the design and PRA analysts. It is only through such a cooperative effort that the models can be developed efficiently, reflect the system design accurately and be most effective in addressing design and operating issues associated with the digital systems.

Section 7: References

1. EPRI 1002835, “Guideline for Performing Defense-in-Depth and Diversity Assessments for Digital I&C Upgrades”, December 2004
2. EPRI 1016721 , “Benefits and Risks Associated with Expanding Automated Diverse Actuation System Functions”, 2008
3. EPRI 1019813 , “Effects of Digital I&C Defense-in-Depth and Diversity on Risk in Nuclear Power Plants”, 2009
4. EPRI 105396, PSA Applications Guide, August 1995..
5. Regulatory Guide 1.174, “An Approach for Using Probabilistic Risk Assessment in Risk-informed Decisions on Plant-Specific Changes to the Licensing Basis”, November 2002
6. ASME RA-S-2009, Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications
7. EPRI 1016731, “Operating Experience Insights on Common-Cause Failures in Digital Instrumentation and Control Systems”, December 2009.
8. NUREG/CR-7007 ORNL/TM-2009/302, "Diversity Strategies for Nuclear Power Plants and Instrumentation and Control Systems"
9. EPRI 1021077, “Estimating Failure Rates in Highly Reliable Digital Systems,” 2010
10. NUREG/CR 0492, "Fault Tree Handbook", January 1981
11. NUREG-0737, Supplement 1, “Clarification of TMI Action Plan Requirements”, January 1983.
12. IEC 61226, “Nuclear Power Plants - Instrumentation and Control Systems Important for Safety - Classification of instrumentation and control functions”, 2009
13. IEC 60880, “Nuclear Power Plants - Instrumentation and Control Systems Important for Safety - Software aspects for computer-based systems performing category A functions”, 2006
14. IEC 60987, “Nuclear Power Plants - Instrumentation and Control Systems Important for Safety - Hardware design requirements for computer-based systems”, 2007
15. IEC-61508, *Functional safety of electrical / electronic / programmable electronic safety-related systems (E/E/PES)*

16. EPRI 1019182, “Protecting Against Digital Common-Cause Failure - Combining Defensive Measures and Diversity Attributes, December 2010.

17. Nancy G. Leveson, "Safeware", Addison Wesley, September 1995

18. EPRI 1022986, Digital Operating Experience in the Republic of Korea, 2011

19. Bickel, J., “Risk Implications of Digital Reactor Protection System Operating Experience”, Reliability Engineering & System Safety, 2006.

20. Yatrebenetsky, M. “Operating reliability of WWER NPP Digital I&C Systems”, ANS NPIC Conf 2010

21. Siu NO, Kelly DL. Bayesian parameter estimation in probabilistic risk assessment. Reliability, Engineering and System Safety1998;62:89–116.

22. NUREG/CR-6928, “Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants”, February 2007

23. http://nrcoe.inel.gov/SparParamEst/WebHelpCCF2010/CCFParamEst2010.htm

24. MIL-HDBK-217F, Department of Defense, “Reliability Prediction of Electronic Equipment, February 18, 1995.

25. RAC, “Nonelectronic Parts Reliability Data”, NPRD-2011, 2011.

26. RAC, “Electronic Parts Reliability Data”, EPRD-97, 1997.

27. NUREG/CR-6962, Traditional Probabilistic Methods for Digital Systems, October 2008

28. ORNL, TM-2006/626,” Industry Survey of Digital I&C Failures”

29. NUREG/CR-4772, “Accident Sequence Evaluation Program Human Reliability Analysis Procedure”, February 1987.

30. EPRI 1020436, “EPRI HRA Calculator 4.1.1”, October 2009.

31. EPRI TR-102348 Revision 1 (NEI 01-01), “Guideline on Licensing Digital Upgrades – A Revision to EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule”, March 2002.

32. NEDO-33201, 'ESBWR Certification Probabilistic Risk Assessment', Revision 6, October 2010.

33. AREVA DCD Tier 2 Rev. 3 Chapter 19 – ‘Probabilistic Risk Assessment and Severe Accident Evaluation’ Section 19.1, August 2011.

Appendix A: Defensive Measures for Digital Equipment

A.1 Fault Avoidance Measures Against Functional Specification Faults

Table A-1 lists a set of fault avoidance measures against functional specification faults and their potential benefits. Such measures 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.

A.2 Measures for Programmable Equipment

Table A-2 provides an example of a set of measures that would be appropriate for programmable equipment. As fault detection measures are usually well known and the object of safety standards (for example, see [18], [20], [23], [24], [25]), the table focuses mostly on fault avoidance measures, and on measures designed to minimize to potential for activating conditions.

A.3 Measures for Smart Devices with Simple, Fixed Functionality

Table A-3 lists a set of 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 [4]. It includes measures to ensure that the device functionality is appropriate for its intended purpose, measures to ensure that the device has a low potential for residual digital faults, and measures to ensure that device failures can be tolerated. While the measures listed in Table A-2 are generally for more complex devices, they may also be useful in simple devices.

Table A-1
Examples of Avoidance Measures against Functional Specifications Faults

Avoidance 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.

Table A-1 (continued)
Examples of Avoidance Measures against Functional Specifications Faults

Avoidance Measures	Benefits
Existence of an unequivocal and easy to reach safe failure position.	Reduce the likelihood of potentially unsafe failures. Ensure rigorous treatment of potentially unsafe conditions (as opposed to abnormal behaviors that cannot result in unsafe conditions, e.g., unspecified behaviors during commissioning tests before fuel is loaded)
Boolean safety outputs with clearly identified failure modes and unsafe failure modes.	
Particular focus on plant conditions for which incorrect or incomplete system specifications could result in unsafe failures (e.g., 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).	

Table A-2
Examples of Defensive Design Features for Programmable Equipment

Defensive Measures	Benefits
Rigorous development and modification processes.	Lower likelihood of introducing faults and higher likelihood of fault detection, resulting in fewer residual digital design faults.
Use of trustworthy tools for development and verification.	
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.	Avoidance of triggering conditions through rigorous identification, characterization and minimization of factors that can influence the functioning of software. Software is confined to well-tested trajectories.
Invariability of software during operation.	
Validation of inputs prior to further processing.	
Clearly identified short term memory.	
Interrupts only for exceptions and clock, no process driven interrupts.	

Table A-2 (continued)
Examples of Defensive Design Features for Programmable Equipment

Defensive Measures	Benefits
Cyclic functioning.	Avoidance of various potential fault triggering conditions. Increased assurance that a safety system CCF is very unlikely to occur with the system in normal "run" mode (checking real-time plant parameters against trip setpoints)
Single-tasking.	
Limited amount of short term memory.	
Asynchronous operation (no internal clock).	
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).	Fault tolerance: software deviations and failures are detected, and the system is rapidly driven to a safe state.
Surveillance of short and long term memory. Defensive programming.	
Rigorous operational procedures for operator requests (one channel at a time, only when absolutely necessary).	Fault tolerance through measures ensuring that digital failures triggered by operator request or elapsed time, e.g., counter or buffer overflows, do not concurrently affect multiple channels or systems.
Staggered startups of redundant channels and diverse systems	
"Dissociation" of Operating System from Application Software.	Avoidance of triggering conditions for Operating System faults, Operating system confined to well-tested trajectories. Plant transients and unanticipated plant behaviors cannot trigger residual faults in Operating System. Improved fault tolerance of Operating System functionality
Transparency of Operating System to plant transients.	
Constant bus loading (processors and communications)	
Further decomposition of Operating System into dissociated modules	
Application Function Library composed of dissociated, simple, stateless, well-proven modules.	Additional assurance that the Application Function Library is very unlikely to contain design faults that could lead to digital failures.

Table A-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.	

Export Control Restrictions

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

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

Together...Shaping the Future of Electricity

Programs:

Nuclear Power

Instrumentation and Control

1025278

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com