Evaluating Commercial Digital Equipment for High Integrity Applications

A Supplement to EPRI Report TR-106439

TR-107339

Final Report, December 1997

Prepared by
MPR Associates, Inc.
320 King Street
Alexandria, Virginia

Principal Investigators
B. Fink
J. Betlack

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

EPRI Project Manager
Ray Torok

Nuclear Power Group, CGD Working Group

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

ORGANIZATION(S) THAT PREPARED THIS REPORT

MPR Associates, Inc.

ORDERING INFORMATION

Requests for copies of this report should be directed to the EPRI Distribution Center, 207 Coggins Drive, P.O. Box 23205, Pleasant Hill, CA 94523, (510) 934-4212.

REPORT SUMMARY

Power plants are increasingly upgrading their instrumentation and control (I&C) systems with commercial digital equipment. The use of commercial software-based devices for high-integrity applications, however, raises new issues in regard to ensuring safety and reliability. Expanding on an approach developed by EPRI for nuclear safety applications, this document provides more detailed guidance for evaluating commercial digital equipment, with an approach that tailors the effort consistent with the importance to safety and plant economics.

Background

In response to growing challenges of obsolescence and increasing maintenance costs, utilities are replacing and upgrading selected I&C equipment. Upgrades typically involve changes from analog-to-digital or digital-to-newer digital technology, with proven commercial products often providing practical solutions. New concerns for high-integrity applications include the potential for common-mode failure of redundant components using identical software, electromagnetic interference (EMI), and, when commercial off-the-shelf (COTS) software is used, the adequacy of the supplier's software development process and documentation. Utilities are using commercial equipment more and more, but their processes for evaluating such equipment to ensure adequate quality are still in the nascent stage. Utilities require a comprehensive, systematic approach for evaluating commercial software-based equipment to ensure safety, reliability, and cost-effectiveness.

Objectives

To supplement TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," with more detailed guidance and examples; to provide a "tool box" of techniques, procedures, and examples that can be applied to specific applications according to their safety significance and complexity.

Approach

An EPRI-sponsored working group of nuclear utility and industry representatives guided the development of this document. The primary focus was addressing digital system issues in context of the "commercial dedication" process used to evaluate and qualify commercial equipment for use in nuclear safety applications. Working group

participation and review by industry representatives and regulators proved invaluable in strengthening and refining the document.

Results

This guideline will help utilities design, evaluate, implement, and obtain regulatory approvals for digital upgrades involving commercial software-based equipment. The guideline emphasizes testing, analysis, vendor assessments, and careful review of operating experience to ensure adequate safety and reliability and to address the associated regulatory issues. This guidance is intended for utilities and other organizations that evaluate commercial-grade equipment for high-integrity applications. The guide references existing industry standards and guidelines and is compatible with utility-specific change processes, including graded approaches for quality assurance. While the guideline is primarily for digital upgrades to nuclear safety systems, it also will be helpful in non-safety and fossil plant applications that require high reliability.

EPRI Perspective

This guideline will help its users avoid problems that nuclear plants and other industries have experienced with digital equipment. TR-106439, the predecessor to this document (which has been reviewed and accepted by the NRC), provides “what-to-do” guidance for nuclear safety-related applications. This document provides more detailed “how-to” guidance, with procedures and examples. Evaluations of commercial digital equipment should consider both safety and economic risk and are appropriate in critical non-safety and fossil plant applications. Control systems can carry significant economic risk, particularly in the face of deregulation. Most often, problems arise because digital devices are treated as "black boxes," with inadequate understanding leading to unexpected and unwanted behaviors. Utilities must have sufficient knowledge of the quality and inner workings of a device to anticipate the types of failures and abnormal conditions that could arise. The need for careful evaluations extends well beyond the domain of nuclear safety systems, and it is hoped that this guideline will receive wide usage in high-integrity applications throughout the industry.

TR-107339

Interest Categories

Plant support engineering
Instrumentation & control
Assessment and optimization
Fossil steam plant O&M cost reduction

Keywords

Digital upgrade
Instrumentation and control
Commercial-grade item dedication
Commercial off-the-shelf software
COTS
Software-based systems

ACKNOWLEDGMENTS

This document was produced with the support of an EPRI Working Group on Use of Commercial Grade Digital Equipment. The successful development of this document is due in large part to the continuing support and encouragement of the working group, and the leadership and direction provided by Bruce Geddes of Baltimore Gas and Electric, the Chairman, and Ray Torok, the EPRI Project Manager. All active members of the working group are listed below. Their support and contributions to this work are gratefully acknowledged.

In addition, special thanks go to several individuals and companies who provided material for inclusion in this report, as well as the benefit of their review and insightful comments on previous drafts. Charles Waite and Bruce Moore of Data Refining, Inc., provided the appendix describing how to do Critical Digital Reviews. Nicolas Henry and Patrick Salaun of Electricité de France contributed information from EDF's research and development program on qualification of digital control systems, including sample test plans contained in the second appendix.

Ray DiSandro of PECO Energy provided anecdotal material from previous digital upgrades involving commercial equipment. Cris Cristallo of Northeast Utilities and Ed Goss of Union Electric also provided information and materials from upgrades that contributed real-world experience and examples to the document. Bill Petrick of Capri Technology, Inc., provided review and input particularly on the subject of requirements definition. And Jim Stewart of the USNRC provided review comments and many useful anecdotes and insights based on his own and other NRC reviewers' experience. Many of these individuals participated not only in the main group meetings, but also in smaller working meetings to brainstorm, review drafts, and provide direction to the authors in developing this guideline. Their input was crucial to producing a useful document.

EPRI Working Group on the Use of Commercial Grade Digital Equipment:

Janardan G. Amin	TU Electric
Jess Betlack	MPR Associates, Inc.
Dave Coburn	Toledo Edison

Cris Cristallo	Northeast Utilities System
Ray DiSandro	PECO Energy Company
Stan Farlow	American Electric Power Service Corp.
Bob Fink	MPR Associates, Inc.
Bruce Geddes	Baltimore Gas & Electric Company
Wayne H. Glidden	Duquesne Light Company
Diljit Gulati	Commonwealth Edison Company
Dennis A. Harris	Triconex Corporation
John Hefler	Pacific Gas & Electric
Nicolas Henry	Electricité de France
Stephan H. Hetrick	MDM Engineering
Timothy E. Hurst	Hurst Consulting, Inc.
Ron Jarrett	Tennessee Valley Authority
Michael Jaeger	Southern California Edison
James T. Keiper	Foxboro Company
John H. Lanier, Jr.	Duke Power
Joseph Naser	Electric Power Research Institute
Ted Quinn	MDM Engineering
Roy Raychaudhuri	Sargent & Lundy
Dave Reigel	GE Nuclear Energy
Fran Rosch	Electric Power Research Institute
Marty Ryan	ABB Combustion Engineering
Patrick Salaun	Electricité de France

Dean Sandlin	Entergy Operations
John G. Sipos	Florida Power Corporation
Brian Steen-Larsen	Pacific Gas and Electric Co.
Jim Stewart	USNRC-NRR
Keith Swing	Raytheon Nuclear, Inc.
Gary Toman	Nutherm International, Inc.
Ray Torok	Electric Power Research Institute

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1

EXECUTIVE SUMMARY

This document provides guidance and tools for the effective application of commercial digital instrumentation and control equipment in high-integrity applications — those that are critical to plant safety, economic performance, or investment protection. This is a supplement to an earlier report, EPRI TR-106439, which established the framework for evaluating and accepting commercial digital equipment.

This section provides a summary of the background, the content of this document and how it can be used, and some of the important messages for the reader. Section 2 describes in more detail the purpose and intended audience for this document, and Section 3 provides a roadmap of the document. It is recommended that all users read these first three sections to obtain a good understanding of the subject matter and how to make effective use of the tools provided here.

1.1 Background

Nuclear utilities are finding they must replace or upgrade their existing instrumentation and control (I&C) systems because of growing problems with obsolescence and increasing maintenance costs. Equipment using digital technology is typically applied due to its ready availability and potential for performance and reliability improvements. Often, commercial products offer the best solution because of their reasonable cost, greater flexibility, and demonstrated reliability. As the base of qualified suppliers of products developed under nuclear quality assurance (10 CFR 50 Appendix B) programs dwindles, utilities are increasingly turning to commercial suppliers for replacement equipment.

With digital technology being introduced into nuclear plant systems, a number of new design and licensing issues have emerged. These include: the use of software and the potential for common cause failure resulting from software errors, the effects of electromagnetic interference (EMI) on digital computer-based systems, and the use and control of equipment for configuring computer-based systems. The industry and NRC have agreed on a framework for addressing these digital issues, described in EPRI TR-102348. The approach emphasizes consideration of the effects of potential failure modes in ensuring equipment adequacy. For software, it stresses the importance of a systematic, well-documented development effort as part of assuring adequate quality.

Commercial products contain pre-existing software that was developed to varying commercial standards, often through a more evolutionary than structured or pre-planned process, and with less documentation than would be required under a 10 CFR 50 Appendix B program. Assurance of quality for these devices comes in part from their application experience and the maturity of the software achieved through its ongoing development and operating history. The need to demonstrate a level of assurance for commercial grade items equivalent to that provided by equipment developed under a nuclear (10 CFR 50 Appendix B) quality assurance program has been well established (10 CFR 21, IEEE 7-4.3.2, EPRI TR-102348). However, a specific approach for evaluating commercial products, developing the needed assurance, and accepting the items for safety-related service, was lacking.

Again, the industry and NRC worked together to reach consensus. EPRI TR-106439 describes how the existing process for commercial grade item dedication (EPRI NP-5652), which has been applied successfully for many years for other types of equipment, can be applied to commercial digital equipment. TR-106439 establishes the framework and provides examples to illustrate how the process can work, typically using a combination of methods outlined in NP-5652: inspection and testing, a survey of the vendor's commercial practices and review of the digital system design, and a review of the product's operating history.

1.2 What Makes Digital Equipment Different: The "Digital Delta"

Commercial digital equipment offers a number of advantages owing to its flexibility, availability, reliability and potential for long-term support. Utilities have installed upgrades using commercial digital equipment that have been very successful, in some cases paying for themselves in the first few years of operation due to increased performance and control capabilities. Commercial digital systems have been found to be more reliable and easier to operate and maintain than some other systems purchased under 10 CFR 50 Appendix B programs.

However, experience has shown that achieving this type of success with commercial digital equipment relies on use of a thorough design, evaluation and acceptance process, as outlined in the licensing and commercial dedication guidelines TR-102348 and TR-106439. The importance of this is probably best illustrated by some of the more painful lessons learned from previous digital equipment installations. A few examples are listed below:

- Digital Feedwater Control System: During the testing of a new digital feedwater control system, the reactor had to be manually tripped because of an unanticipated runback of the reactor recirculation pumps. The cause was found to be a software coding error.

- Digital Turbine Control System: A software logic error caused an improper turbine runback and plant transient.

- Microprocessor-based Overhead Annunciator System: The overhead annunciator system failed and a plant alert was declared as a result of a command being typed incorrectly at a configuration terminal. The incorrect command triggered an undocumented software feature that caused loss of alarm processing without notification to the operators.

- EDG Load Sequencer: The EDG load sequencer failed to start during a surveillance test. The cause was a software logic error.

- Digital Feedwater Control System: During full power operation, a commercial controller used in the new digital feedwater control system began opening a feedwater valve, causing the steam generator level to rise. An EMI problem had triggered an internal error that halted the processor, disabled the manual control, and let the output drift. The controller would not allow operators to take manual control so the plant had to be tripped.

Digital equipment often appears simple, but this can be deceptive. For example, a single programmable logic controller (PLC) that is installed to replace a cabinet full of relays looks like a simplification of the system, and it is, from an "outside the box" standpoint. But in fact, the PLC itself may harbor a great deal of complexity "inside the box," in its hardware (chips incorporating millions of transistors), software (firmware with many thousands of lines of code) and internal system architecture that determines how information flows through the equipment (task scheduling, memory sharing, self-testing, interrupt handling, etc.). There are several key results of this:

- Whereas adequate performance of an analog electronic circuit or relay logic circuit often can be verified solely by testing, this is not true for most digital equipment.

- Verifying adequate quality of a digital product typically requires gaining an understanding of the process actually used by the vendor in producing the software.

- Digital equipment can exhibit subtle and unexpected behaviors and failure modes, which can result in more severe and difficult to predict consequences as compared to the original analog or discrete component-based system.

It is important for anyone undertaking a digital modification or replacement to understand the fundamental differences between digital and analog electronic equipment. These differences can impact the performance and failure modes of the equipment, and the methods and techniques required to evaluate and accept the

equipment for installation in the plant. The differences are referred to here as the "digital delta."

1.3 Summary

This document provides more detailed guidance and "how-to" information to supplement the higher-level guideline, TR-106439. This second-tier document is intended to be used as a "toolbox" of useful information, examples, and sample materials to help utilities make use of commercial grade digital equipment. It provides guidance on defining a digital upgrade project, including planning for activities that will be required to evaluate or dedicate commercial equipment. It contains guidance and tools to support testing, surveying a vendor's process for developing commercial equipment, performing critical reviews of the design, and evaluating operating history of the equipment. Examples and case studies are provided to illustrate how these materials can be applied. The focus is on the "digital delta" -- the differences in the evaluation and acceptance process that are required because the equipment is digital.

Also, like TR-106439, this document focuses primarily on dedication of commercial grade digital equipment for nuclear safety applications. However, the information also can and should be used for important nonsafety-related applications, particularly those that are critical to maintaining plant power operation, personnel safety, or investment protection. Although the emphasis is on analog-to-digital conversions or upgrades to I&C systems, the guidance and tools given here also can be applied when replacing existing digital equipment with new, commercial digital products (digital-to-digital changes).

Section 2 describes the intended audience for this document. Broadly stated, the audience includes utility engineers, managers, licensing, procurement, vendor auditors and other personnel involved in the evaluation and acceptance of commercial digital instrumentation and control equipment. Section 3 provides an overview and roadmap of this document. The roadmap, plus the index provided in Section 8, are intended to allow each reader to quickly get to the information needed.

1.4 Important Messages

There are a number of important messages that can be obtained from this document and the upper-tier guideline, TR-106439. These are summarized below.

Messages for Engineers

There are several important messages in this document for engineers who are involved in digital upgrades. To summarize:

- Commercial grade digital equipment can be used effectively, but only if carefully evaluated and properly applied. There is no cookbook, but the framework and guidance of TR-106439, plus the more detailed information contained in this document, provide tools necessary to do the job.

- Commercial digital equipment should not be treated as a "black box." This has been the source of many of the problems experienced in plant installations. For both cost and safety reasons, users of this equipment should have sufficient knowledge of the inner workings to anticipate the types of failures and abnormal conditions that can arise from its use.

- Be careful with cost/benefit assessments. The evaluation and acceptance activities can easily cost far more than the digital device. Make sure you understand what you're signing up for when you decide to go with a commercial product.

Messages for Managers

In addition to ensuring that engineers who will be involved in digital upgrades receive and understand the messages listed above, there are some important messages for management here as well:

- If you decide to go with a digital upgrade, be prepared to commit the resources needed to do the job right. Cutting corners up front can easily result in much larger cost implications later if problems arise.

- Make sure that people with the required expertise are applied to the project. Everyone involved in the project does not have to be a computer scientist (just as all members of a project involving complicated materials issues do not have to be metallurgists). However, project team members should have at least a basic understanding of the technology, and the team should know when specialized expertise is required and either have it or know how to get it. The needed expertise may be obtained by using personnel from another department, by hiring consultants or contractors, or through training and in-house development. As a minimum, a project involving commercial digital equipment typically requires a cooperative effort among procurement, design, and vendor audits personnel to be successful.

- Experience has shown that something like a "culture change" must occur within the organization to develop an awareness of digital equipment issues and a comfort level appropriate to deal with them. Awareness includes recognizing when digital equipment or parts are involved in a plant modification or maintenance action (e.g., a microprocessor with firmware embedded in some new switchgear being installed, or in a valve actuator replacement).

- Significant benefits can be obtained by utilities sharing information or pooling their resources in performing dedications. This can make evaluation and acceptance of commercial digital equipment much more cost-effective than each utility going it alone.

.

2

PURPOSE

2.1 Audience

This document is intended for use by utility design and procurement engineers, vendor auditors, licensing personnel, and managers who are involved in or responsible for the application of commercial digital equipment. It focuses on specific issues and topics associated with applying commercial grade *digital* equipment. It is assumed that the reader is already familiar with the more general subjects such as dedication of commercial grade items in general, preparation of a modification package, etc. Also, this document does not attempt to educate the reader on technical subjects that are covered elsewhere (e.g., EMI, V&V). At the same time, specific knowledge or experience with digital upgrades or replacements is not necessary in order to use this document.

Refer to EPRI TR-102348, TR-106439, and other appropriate references for definitions of terms used in this document that may be unfamiliar.

2.1.1 Utility Design, Procurement and Licensing Engineers and Auditors

Engineers involved in both design and procurement should find information here that will help them do their jobs when those jobs involve the use of commercial grade digital equipment. As pointed out in TR-106439, it is important that both design and procurement activities work together to evaluate and accept this type of equipment.

Vendor auditors who may be called upon to perform commercial grade surveys for digital products will find useful information in this document. Finally, licensing engineers may also find this document useful as a supplement to the licensing guideline, TR-102438, and the upper-tier commercial grade document, TR-106439.

2.1.2 Utility Managers

It is important for utility management to understand both the benefits and the potential problems associated with the use of commercial digital equipment, and the process involved in evaluating and accepting such equipment for use in the plant. Managers and others who will be involved in some way with these projects (e.g., operations and

maintenance personnel) should gain a basic understanding of the upper-tier guideline, TR-106439, and should read at least the first three sections of this document.

2.2 Objective

The objective of this document is to provide more detailed "how-to" guidance to supplement TR-106439, and a "tool box" of useful information and materials to assist utilities in the use of commercial grade digital equipment. The materials that are provided here are not intended to present the *only* way of accomplishing their respective tasks. As a user of these materials, you may disagree with some of the details or find other ways that you consider are better suited for your project. The goals are to obtain the needed assurance as defined in 10 CFR 21 and TR-106439, to avoid problems or surprises when the equipment is placed in service or during its life cycle, and to contain costs. This document is just a toolbox — each user must decide the appropriate use for the tools provided.

2.3 Suggested Reading

Design and procurement engineers who will be directly involved in a digital upgrade using commercial equipment should be very familiar with the upper-tier guideline TR-106439, as well as the EPRI licensing guideline (TR-102348) and the commercial grade item dedication process as described in EPRI NP-5652 and the regulation 10 CFR 21.

In addition, all readers will benefit from some exposure to the following reading materials that provide general background and lessons learned on the application of digital equipment, and information on the licensing issues and NRC review process for digital upgrades:

- *Safeware, by Nancy Leveson.* This widely read text describes in much more detail the problems that can be encountered with computer-based systems in safety applications, and why they occur. It discusses why traditional quality assurance methods are not adequate by themselves, and the importance of failure/hazards analysis in developing safe systems. The book provides many anecdotes and actual case histories that serve as useful background reading for this subject.

- *"Digital Instrumentation and Control Systems in Nuclear Power Plants — Safety and Reliability Issues," by the U.S. National Research Council.* This report describes the licensing issues associated with the use of digital I&C systems, gives background on the interaction between utilities and the USNRC on this subject, and for the eight most prominent issues provides discussion and recommendations. One of the issues is the use of commercial off-the-shelf (COTS) equipment.

- *Appendix 7.0-A of the Standard Review Plan (NUREG 0800) Chapter 7, "Review Process for Digital Instrumentation and Control Systems."* This appendix to the introductory part of Chapter 7 on I&C systems describes NRC's updated review process for digital I&C systems.

3

OVERVIEW AND ROADMAP

The purpose of this overview is to help the reader understand how this document is organized, and more importantly, to assist the reader in quickly finding material that will be helpful with a specific task.

Figure 3-1 provides a roadmap to the document. As shown in the figure, the sections are organized roughly according to the process involved in defining the project, identifying commercial equipment and its requirements, defining critical characteristics for the equipment, and verifying those characteristics using the methods established in NP-5652. Guidance is provided for each of these phases of the process, supplementing the higher-level guidance in TR-106439.

Also, a version of the flowchart from TR-106439 which links the content of this document to TR-106439 and other higher-level EPRI guidelines is provided in Figure 3-2. It indicates which portions of the process in TR-106439 are supported in this document, and provides pointers to the sections in this document where the various process steps and topics are covered. Note that this document does not address Technical Evaluation of Replacement Items (see EPRI NP-6406). Also, it does not specifically address licensing and 10 CFR 50.59 evaluations (see EPRI TR-102348). However, as shown by the gray bars in Figure 3-2 and described in TR-102348, licensing interacts with essentially all of the other activities shown in the figure and described in this document.

Activities to support dedication of commercial digital equipment should be identified and planned early in the project, so as to avoid costly surprises later. Section 4 provides guidance on the project definition and planning process. The flowchart shown in Figure 4-1 maps out the project definition activities and provides an overview of the process. Supplemental guidance is included on grading, evaluating complexity, and doing cost-benefit evaluations.

Section 5 supplements the guidance of TR-106439 in several key areas including the definition and verification of critical characteristics, preparation of procurement specifications, and testing. Additional guidance is also provided on performing vendor surveys and design reviews, and on the use of operating history.

Section 6 provides examples that supplement those provided in TR-106439. They illustrate application of the guidance given in this document and in the higher-level

guideline. The examples range from a fairly simple controller application to the upgrade of a portion of an Engineered Safety Features Actuation System (ESFAS).

References are given in Section 7, and Section 8 contains an index that can be used to find discussion of specific topics addressed in this document.

Finally, two appendices are provided. Appendix A gives detailed "how-to" guidance for performing critical reviews of digital products and vendors. Appendix B presents some sample test plans for evaluating timing issues associated with digital control systems. These appendices are introduced in Section 5.

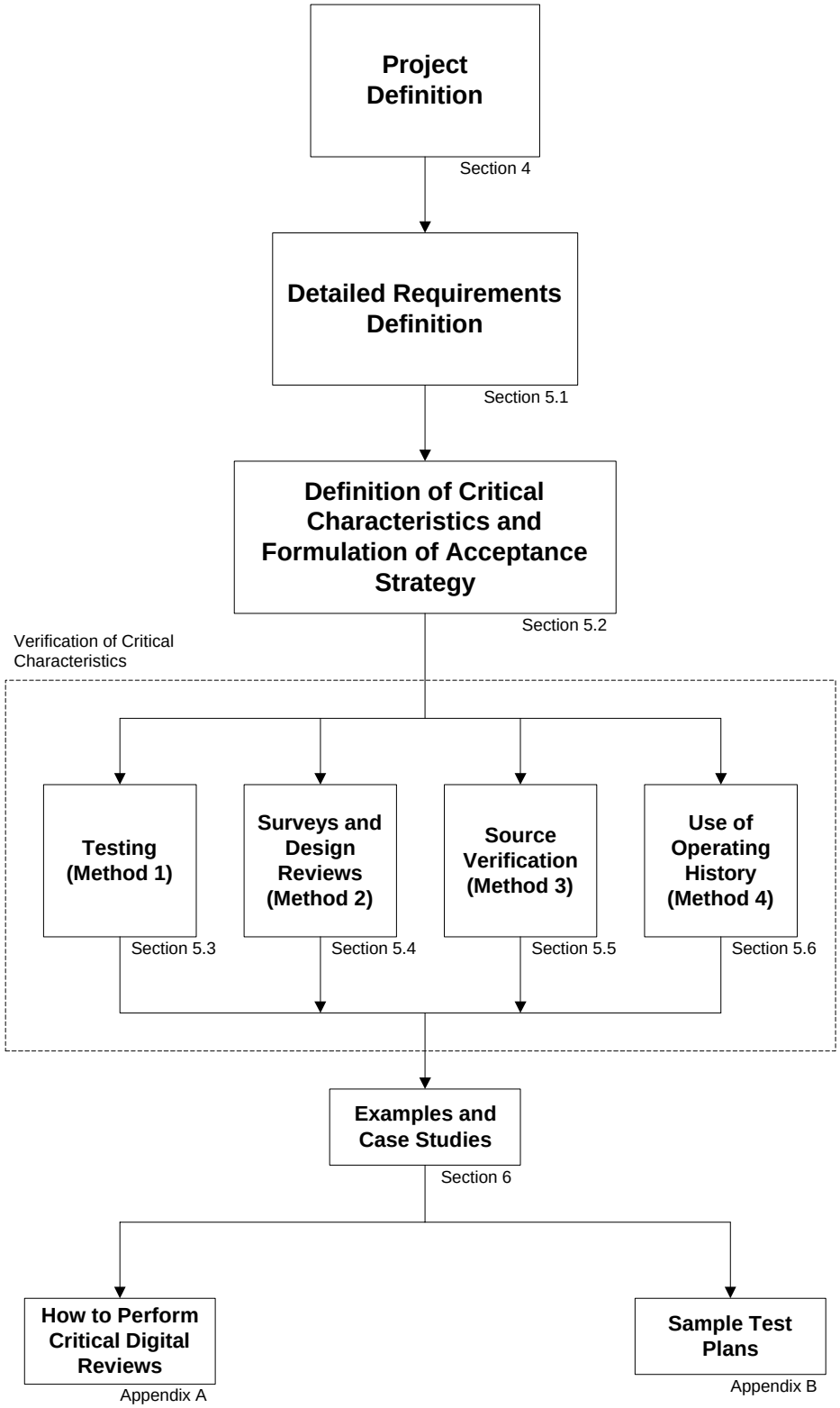


Figure 3-1
Roadmap of Tier 2 Document

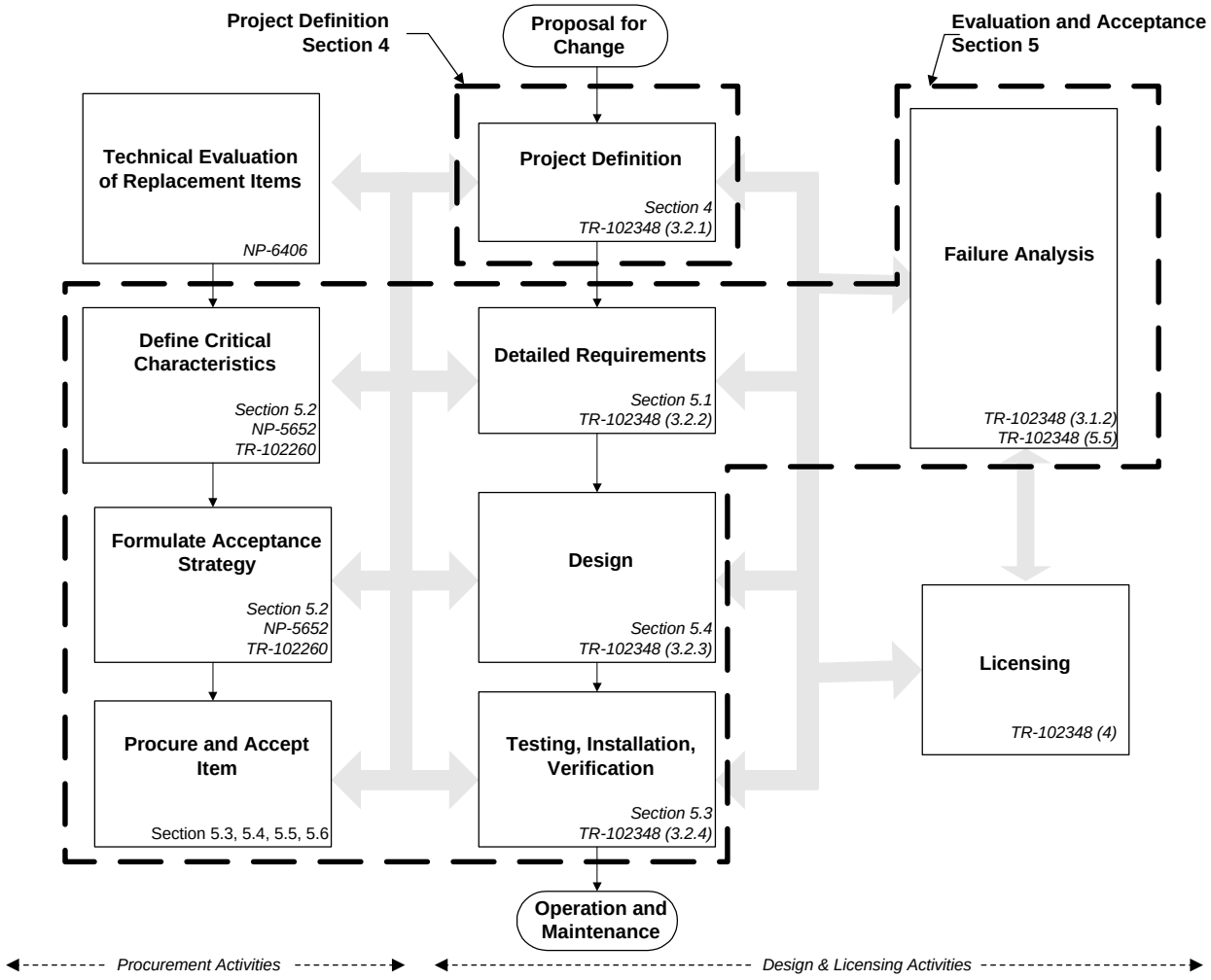


Figure 3-2
Relationship of Tier 2 Document to Higher-Level Guidelines

4

PROJECT DEFINITION

Project definition is particularly important for digital upgrades, which typically require more up-front effort to get a complete picture of the total required effort and cost to complete the project, and to avoid surprises that can have a major impact on the project's schedule and budget. This is especially true when commercial equipment is being considered. Reasons for the increased up-front effort include:

- There is a wide range of activities that may be required to complete the dedication of commercial digital equipment, and thus a wide variation in cost and schedule associated with these activities. As described in EPRI TR-106439, the safety significance and complexity of the equipment and the application determine the scope of activities required to accept the equipment — this is referred to as a "graded approach." When defining the project, an ***initial grading*** based on safety significance and complexity is important in planning the project and estimating costs.

- If commercial equipment is to be used, there is potential for the dedication activities to uncover shortcomings in the equipment or the vendor's practices that could lead to additional work for the utility to complete the dedication. In extreme cases, the utility may have to abandon that vendor/equipment and start over with another product. Thus it is important to do some ***screening of products and vendors*** prior to committing to the project, and to the cost and schedule estimates.

This section provides guidance on project definition for cases in which commercial digital equipment may be involved in the upgrade. For our purposes here, project definition refers to all the activities performed up to the point of making a commitment to the project, with budget and schedule established and equipment options narrowed and well-defined.

4.1 Flowchart of Project Definition Activities

The flowchart shown in Figure 4-1 maps out the project definition activities and provides an overview of the process. Each of the activities identified in the flowchart is discussed in the subsections below. Examples of project definition activities and specific cases in which these activities have or have not been applied are provided.

Most of these are taken from the examples of Section 6. As indicated in the flowchart, the project definition process involves iteration to arrive at a well-defined design concept and a selection of components that offer the best solution option.

4.2 Pre-Conceptual Design

The first step of the project definition phase is to clearly define the objective(s) of the modification or replacement and establish early design concept(s). We refer to this as "pre-conceptual" because in some organizations, conceptual design is a formally defined phase of the design effort. Here, we are talking about the early concepts that are formed as the objectives of the change are defined. EPRI TR-102348, "Guideline on Licensing Digital Upgrades," points out that the plant systems and associated components that will be involved in the upgrade should be clearly defined early in the process. Key activities at this stage of the design process involve defining:

- Objective(s) of the modification: Determine what the modification is intended to accomplish. Clearly define any increase in functionality planned for the upgrade relative to the existing system.
- System(s) to be modified: Identify the systems or components that will be modified to support the objectives.
- Other systems affected: Identify the effects from this modification on other systems or components and determine the interfaces affected.
- Early design concepts: Define the basic concepts for design(s) that would be expected to fulfill the objectives.
- High risk areas: Identify important system-level failure modes and high-risk areas that should be considered in the conceptual design and other downstream activities. This is the beginning of the failure analysis activity that will continue throughout the design definition, implementation and verification process (see Figure 3-2).

Missing a High-Risk Area

At one plant, a new digital feedwater control system was installed with improved functionality and a new human-machine interface. Shortly after it went into service, a condition occurred that caused the system to shift from automatic to manual control. Unfortunately, the system provided little indication to the operators that this had occurred. They did not detect the change, and the result was a plant trip.

This was a case in which a high-risk area had not been identified up front and considered in the design. The possibility of a switch to manual without adequate operator indication could have been identified as a risk, and appropriate actions taken in the requirements and the design to prevent it.

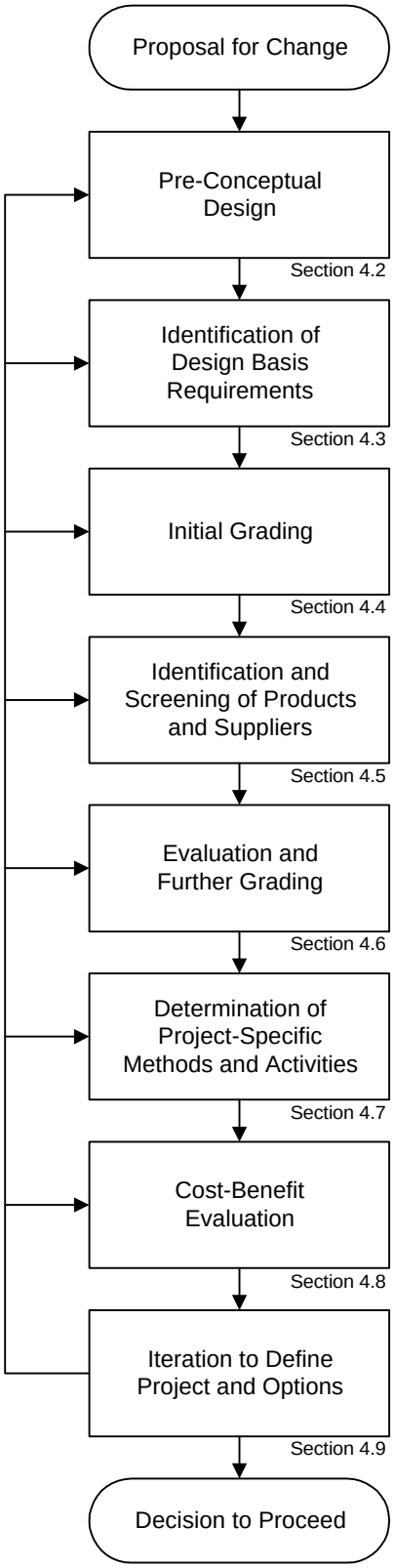


Figure 4-1. Flowchart of Project Definition Process

As the upgrade increases in complexity and safety significance, so will the amount of pre-conceptual design effort. This can be seen in the graded sequence of examples provided in Section 6. In Example 6.1, a fairly simple indicating controller replacement, the objective of the upgrade is simply finding an available indicator to replace one which is no longer supported by the vendor. The indicating controller performs only two functions, one of which is nonsafety-related, and the controller is already used in other plant applications. As a result, the pre-conceptual design activities are not very extensive.

In contrast, Example 6.4, which involves a relatively complicated monitoring system (ICCMS) using one main processor plus multiple other microprocessors to perform several safety-related monitoring functions, required substantially more pre-conceptual design effort. Defining the specific monitoring functions to be replicated and what enhancements would be made, determining the interface with the plant computer system, and deciding whether any process inputs or outputs would be changed represented a significant effort by comparison to the simpler example.

4.3 Identification of Design Basis and Licensing Basis Requirements

Understanding the design basis and licensing basis requirements for the system and the equipment being modified or replaced is necessary in order to assess the safety significance and select a design approach for the upgrade. This will help to grade the efforts applied in downstream activities.

10 CFR 50.2 defines "design bases" as *that information which identifies the specific functions to be performed by a structure, system, or component of a facility, and the specific values or ranges of values chosen for controlling parameters as a reference bounds for design. These values may be (1) restraints ... or (2) requirements derived from analysis....*

10 CFR 54.3 defines "current licensing basis" (CLB) as *the set of NRC requirements applicable to a specific plant and a licensee's written commitments for ensuring compliance with and operation within applicable NRC requirements and the plant specific design basis (including all modifications and additions to such commitments over the life of the license) that are docketed and in effect. The CLB includes the NRC regulations ... and appendices thereto; orders; license conditions; exemptions; and technical specifications. It also includes the plant-specific design-basis information defined in 10 CFR 50.2 as documented in the most recent final safety analysis report (FSAR) ... and the licensee's commitments .*

Source documents for design and licensing basis requirements include the following:

- Final Safety Analysis Report (FSAR)
- FSAR updates
- License commitments to Regulatory Guides, Branch Technical Positions, and other regulatory documents
- Plant Technical Specifications
- Industry codes and standards
- System descriptions
- Equipment design documents
- Calculations
- Specifications
- Design basis documentation packages
- Specific license commitments or provisions which might address specific issues, e.g. any provisions relating to diversity and common mode failure.

4.4 Initial Grading

As illustrated in Figure 3-2 of EPRI TR-106439, and stated in 10 CFR Part 21, the goal of dedication is to "provide reasonable assurance that a commercial grade item . . . will perform its intended safety function and, in this respect, is deemed equivalent to an item designed and manufactured under a 10 CFR Part 50, Appendix B, quality assurance program." Thus the judgment that an adequate level of assurance has been reached is based on achieving equivalency to nuclear grade equipment (equipment developed under a 10 CFR 50 Appendix B program).

The key question is, given the equipment's importance to safety (and plant operability/investment protection when we widen our view to include important nonsafety-related equipment), what are the appropriate scope and level of detail or rigor required to obtain reasonable assurance that the item is equivalent to one developed under 10 CFR 50 Appendix B? TR-106439 recommends that a graded approach be used, tailoring the scope and rigor of these activities according to the safety significance and complexity of the equipment and its application.

The regulatory basis for using a graded approach based on safety significance derives from 10 CFR 50 Appendix B, which states, "The quality assurance program shall provide control over activities affecting the quality of the identified structures, systems and components, to an extent consistent with their importance to safety."

4.4.1 Graded Approaches

The use of a graded approach is consistent with a number of standards and methods that have been developed to categorize systems and assign degrees of rigor associated with addressing quality issues for the system or component. Examples of these are contained in the following references:

- EPRI TR-103291, the EPRI V&V Handbook
- IEC 1226
- IEC 1508 Draft
- ISA S84.01
- NUREG 800, Standard Review Plan
- NUREG/CR-6421

The EPRI V & V Handbook suggests a graded approach be used in determining the scope and rigor of verification and validation activities applied in software development. The approach first classifies the system in which the software will be used, based on its importance to safety. This results in assigning the system to one of four categories (A, B, C, or D). Then adjusting factors are applied based on several factors including complexity, availability of diverse backups, etc. These are used to arrive at a software classification and one of four corresponding software integrity levels (1, 2, 3, or 4). Finally, the handbook recommends different types of activities, and levels of rigor, for verification and validation of software at each of the defined software integrity levels.

The draft international standard IEC 1508 is receiving a great deal of attention because of the widespread use of IEC standards. IEC 1508 is intended to be applicable to all application sectors, not just nuclear power. Its primary focus is on safety-related control systems incorporating electrical/electronic/programmable electronic (E/E/PES) devices. IEC 1508 relies on a related standard, IEC 1226, which classifies systems based on importance to safety. IEC 1508 then specifies Safety Integrity Levels for E/E/PES safety-related systems based on associated levels of risk (e.g., probability of failure to function on demand). Four Safety Integrity Levels are defined using this risk-based approach. Requirements are established for system architecture, scope and

rigor of activities such as V&V, etc., based on the required Safety Integrity Level. This is similar to the approach used in the EPRI V&V Handbook.

The primary standard that specifies requirements for nuclear plant safety systems in the U.S. is IEEE 603. New safety system designs that are committed to this standard must meet all the requirements in the standard, but IEEE 603 does not specify the scope and rigor of the verification activities needed to demonstrate this. Chapter 7 of the NRC's Standard Review Plan, NUREG 800, applies a level of grading by singling out the Reactor Protection System and Engineered Safety Features Actuation System (RPS & ESFAS) for special review requirements beyond those applied to other safety systems. However, the SRP does not go beyond this in specifying different scope or rigor of verification activities for different safety-related systems.

Some U.S. plants have established pilot programs for applying graded quality assurance to nuclear plant systems using risk-based approaches. However, these have not yet been implemented on a widespread basis.

4.4.2 Grading Applied to Dedication of Commercial Digital Equipment

Figure 4-2 shows how a graded approach can be applied in evaluating and accepting commercial grade digital equipment, amplifying the high-level guidance in EPRI TR-106439. For each step in the process, examples of the inputs that may be used are shown in the figure. (These are examples only and are not intended to be all-inclusive.) Each step in the process is discussed briefly below.

Determine Safety Significance

The first two steps in the process determine the safety significance of the commercial grade item being evaluated. This begins by identifying the safety significance of the plant system or component in which the commercial grade item will be used, or which will be affected by the item. For example, if an individual controller is being replaced in a plant control system, the safety significance of the control system needs to be determined. The plant's QA program (including a graded QA program if one exists) is a primary input to this determination. Other inputs may include the plant Technical Specifications and other licensing commitments, and the Standard Review Plan. Also, some plants make use of a probabilistic risk or safety assessment (PRA/PSA) in determining the safety significance of plant systems and components.

With the system's safety significance established, the safety significance of the specific commercial grade item needs to be determined. This depends on the safety function of the equipment, as determined by a technical evaluation (e.g., see EPRI NP-6406), and the results of the initial failure/hazards analysis. At this stage of the project the failure analysis will be primarily at the system level. It can determine the potential

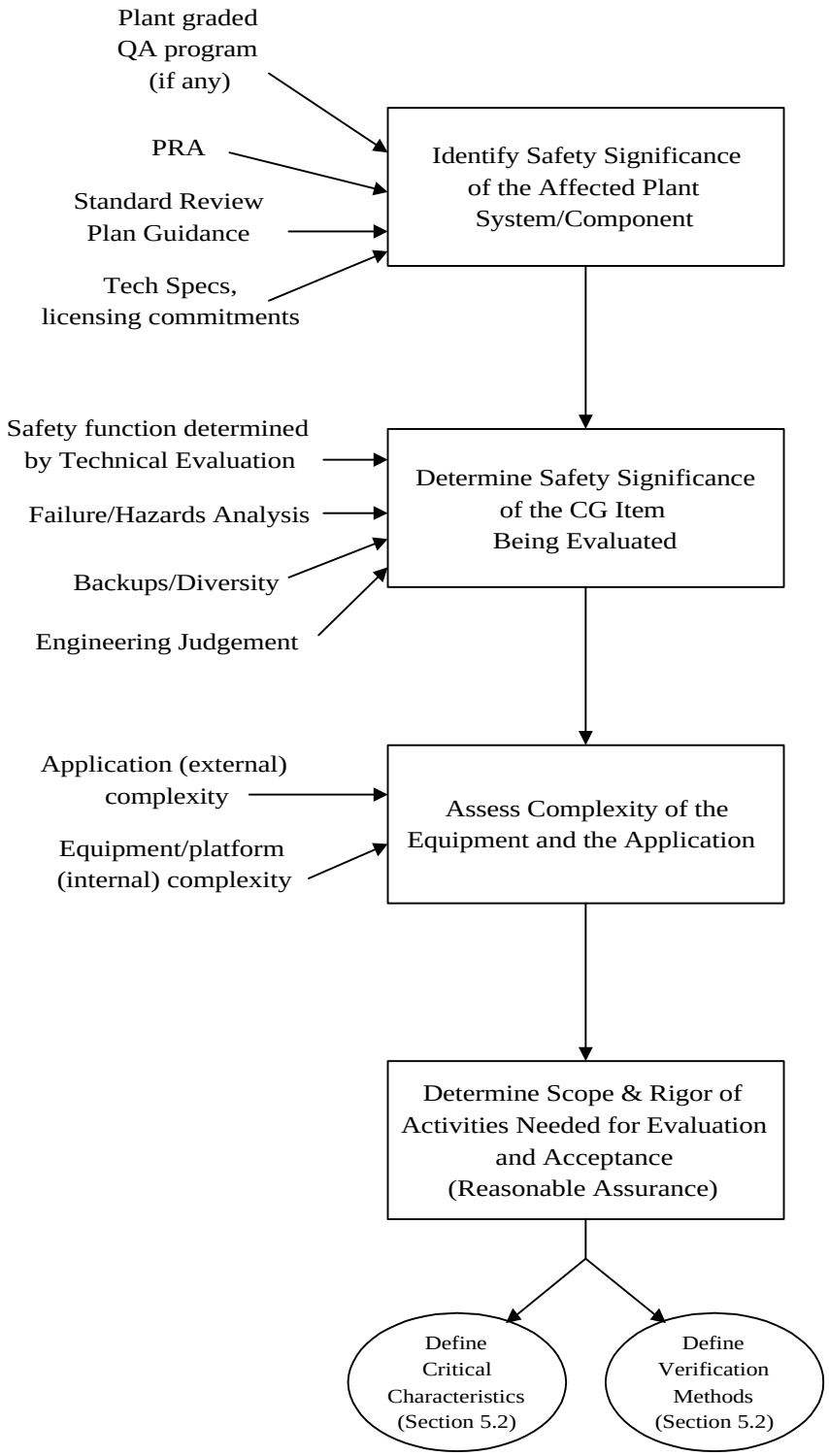


Figure 4-2. Graded Approach Based on Safety Significance and Complexity

consequences of failures of the commercial device, based on the effects of those failures on the system and the plant. The availability of backups or other diverse means of accomplishing the function also should be considered. Finally, because these considerations typically are somewhat subjective, the determination of safety significance relies on engineering judgment.

Assess Complexity

The complexity of the equipment and the application are assessed next. At this point the internal complexity likely will not be known — this will be revisited later when a specific device and vendor are known. The application complexity may be somewhat better known at this stage. In both cases, whatever information is available should be used to make an initial assessment. Complexity is discussed in more detail in Section 4.6.

Make Initial Determination of Scope and Rigor of Activities Required

Finally, based on the safety significance and complexity, the appropriate scope and rigor of activities likely to be needed for evaluation and acceptance (to obtain reasonable assurance) are determined. This will provide input to the definition of critical characteristics and specific verification methods to be applied.

It is difficult to define rigid classification rules for this process because there typically are a number of methods and activities available that can be used to verify specific critical characteristics. Often the choice of which methods to use and the level of rigor to be applied in one area will depend on the findings in another (e.g., the degree to which documented operating history is pursued may depend on the strength of the findings from the vendor survey). Also, classification of commercial digital equipment according to complexity of the platform and the application can be quite subjective. In the end, engineering judgment is required to determine the most appropriate combination of activities to reach the required level of assurance.

The examples in EPRI TR-106439 and in Section 6 of this report illustrate application of the graded approach. In the examples, the type and number of critical characteristics chosen and the methods of verifying the critical characteristics are selected based on the safety significance and complexity of the device or system involved.

It should be noted that this graded approach is consistent with the guidance the NRC uses in reviewing commercial grade item dedications. NRC Inspection Procedure 38703 offers the following guidance for NRC reviewers:

> *Criterion II of Appendix B to 10 CFR Part 50 provides for the application of quality assurance over activities affecting the quality of structures, systems, and components to an extent consistent with their importance to safety. The application of graded quality*

assurance to the CGI dedication process should include consideration of the item's importance to safety and the factors specific to the item being procured. Certain items and services may require extensive controls throughout all stages of development while others may require only a limited quality assurance involvement in selected phases of development. The following factors should be considered in determining the extent of quality assurance to be applied:

- *The importance of malfunction or failure of the item to plant safety,*
- *The complexity or uniqueness of the item,*
- *The need for special controls and surveillance over process and equipment,*
- *The degree to which functional compliance can be demonstrated by inspection and test, and*
- *The quality history and degree of standardization of the item.*

Additional guidance on the use of graded quality assurance can be found in the non-mandatory appendix to ANSI N45.2.13-1976.

4.4.3 Initial Grading to Support Identification and Screening of Products/Suppliers

At this stage of project definition, the design and licensing bases for the system and the specific needs for any commercial components should be reasonably well known. Also, there should be at least a preliminary assessment of the complexity of the application. This allows some initial grading that can be important in the process of identifying and screening potential products and suppliers (next section). Further grading and evaluation of equipment complexity are discussed in 4.6 below.

4.5 Identification and Screening of Potential Products and Suppliers

Identifying available products that will meet the project needs is a normal part of project definition. This activity is especially important when commercial grade components are to be used. One advantage of using commercial grade components is that there is a larger number of candidates available. However, the larger variety also creates the need for more screening effort. Accordingly, it is important to do an initial screening of the products and the vendors/suppliers to make an early determination of their viability for this application. Examples of screening questions that might be used include:

- Does the vendor have a written quality assurance program? Is there a separate quality assurance organization within the company?

- What industry standards (e.g., ISO 9000) does the vendor follow in software development and quality assurance?
- What software V&V methods are used?
- Will the vendor support a survey?
- When was the software/firmware used in this product originally developed? How much is new versus "legacy" code?
- What software development documentation is available for review?
- What mechanism does the vendor provide for error reporting?
- What approach does the vendor use for software configuration management? What standards does the vendor conform to?
- Will the vendor allow access to source code for reviews or walkthroughs?

Vendor published literature and product specifications will answer some of the questions that need to be addressed. For example, literature and product specs probably:

- Explain the vendor's intended usage for the product, or vendor expectations regarding its use.
- Describe the characteristics that the vendor likely controls in the manufacturing process.
- Describe testing, e.g., MIL Standard tests of system components.
- Provide some of the device performance characteristics.
- Provide some of the device physical characteristics.

Using a Previously Dedicated Product

Example 6.4 describes a case in which a main processor unit had to be selected that would provide all the required functional capabilities for a complex monitoring application, and would be likely to make it through dedication successfully. The unit that was chosen was one that had been dedicated previously by an owners group for another safety-related application. This avoided repeating the entire dedication effort for the main processor, and took advantage of the operating experience gained in the previous application. This early planning saved time and money and also took advantage of available operating history.

Vendor literature and specifications will probably not:

- Provide adequate information about the quality of the process used in developing and controlling the manufacture of the product.
- Provide adequate information for verification of dependability critical characteristics.
- Provide sufficient operating history information to address application specific issues.

Obtaining initial information on the product's track record can be helpful at this stage. Vendors will normally provide lists of customers who are using a product. Telephone conversations with and/or visits to a few customers can provide valuable product performance information. Actual users of the product are more likely to identify any weaknesses in the product's capabilities or performance history. Section 5.6 discusses use of operating history in more detail.

Sources of information other than product literature and contacts with vendors and their customers include:

- NUPIC audits/surveys, and NUPIC meetings
- Other utilities' applications of the product or dealings with the vendor. Discussions with personnel at other plants who use the product can provide valuable information on a product's performance and reliability.
- Joint Utility Task Group (JUTG) meetings and surveys, and the JUTG CGI database
- INPO NPRDS and the more recent "EPICS" system, NRC Information Notices, Part 21 Notices, etc.
- Nuclear Materials Management Exchange (NMME) meetings
- Initial look at the product's operating history, based on experience in other applications (including applications at this plant or in the utility's fossil plants, as well as others' experience) — if there is bad experience out there, it is important to make an initial attempt to unearth it now, before committing the project to that particular product.

Results of the initial screening should include:

- Identification of viable equipment options including commercial grade and 10 CFR 50 Appendix B equipment suppliers.
- Initial information on the products and vendors, which may be useful later in supporting evaluation and acceptance of the equipment.
- A short list of preferred equipment and vendor options.
- Determination that "short list" vendors will support a utility audit or survey of their QA, design and implementation processes.
- Determination that the "short list" vendors are "healthy" and can be expected to exist and support their products for the next several years.
- Determination of what formal QA programs, e.g., ISO-9000, and formal design processes the "short list" vendors have in place. Whether or not a vendor has a formal QA program and the type of program provide some indication of the likelihood that a survey will find the vendor acceptable.

4.6 Evaluation of Complexity and Safety Significance and Further Grading

Section 4.4 discussed the graded approach, illustrated in Figure 4-2, and an initial look at grading. At this stage, with some of the vendor and equipment options better defined, further grading can be accomplished including a more thorough evaluation of complexity.

4.6.1 Continuing the Failure Analysis

At this stage in the process, with some of the specific equipment/product options identified, the failure analysis can look at external failure modes of the equipment and relate these to the system-level evaluations already performed. (Internal failure modes of the equipment are not likely to be known in detail at this point in the process — this will be revisited later when the chosen product is evaluated in more detail.) The initial look at failure modes can assist in selecting the design approach and better defining the equipment options. Also, early failure analysis can identify important design criteria and possible mitigation strategies, which can affect the definition of critical characteristics and verification methods to be used and may affect the design.

For example, see the digital feed pump governor anecdote presented in Section 5.7. In that example, the utility recognized early in the project that a common mode software failure in the new governors could result in a system-level failure mode that was

significant to plant safety, and was previously unanalyzed. It was decided that the most cost-effective way of treating this was to add an independent circuit to the modification that would detect this condition and take appropriate mitigating actions. This was considered the preferred alternative to performing additional reviews and verifications of the governor software to ensure that the common mode software failure of concern would not be likely to occur during the plant life.

4.6.2 Evaluating Complexity

Another appropriate activity at this stage of the project is to take a first look at the complexity of each design option. This should be viewed from the standpoint of the digital system (e.g., the differences between a single controller, several intercommunicating PLCs, and a distributed control system) and the digital equipment/components to be used. Some specific factors that should be addressed in assessing complexity include:

System/Application Complexity Factors

Examples of factors to consider include:

- Number and complexity of functions performed
- Number and complexity of operator and other human-machine interfaces
- Number of inputs, outputs, and interfaces with other systems or components
- Number and complexity of device interconnections within the system

Application/Platform Complexity

Examples of items to consider for the application/platform are listed below. Note, however, that at this point there may be insufficient information to evaluate many of these factors in detail. Some of the information may be obtained only after the project has committed to performing a commercial grade vendor survey and design review (see Section 5.4). At this stage in the process, an initial assessment should be made so that appropriate decisions can be made regarding the scope and rigor of the dedication activities that will be required. Complexity and the factors listed here should be revisited when more detailed information becomes available later in the process.

- Number of microprocessors involved; note that the number may not be evident from the vendor literature
- Number of functions that can be performed by each microprocessor

- Internal device communications (e.g., passive backplane or more complex communications among components)
- Number of distinct software components involved and their inter-relationships
- Amount/size of software code
- Number of "function points"
- Complexity of the internal, real-time system architecture (e.g., considering the operating system and items such as multitasking, dynamic memory allocation, scope and complexity of self-diagnostics, etc.)

4.6.3 Keep it Simple!

Avoiding unnecessary complexity and keeping the system as simple as possible will minimize up-front costs, save time and effort throughout the development process, and make the system/equipment easier to operate and maintain throughout its lifetime.

Eliminating "bells and whistles" is very important in avoiding unnecessary complexity. One of the advantages of digital equipment, particularly commercial products, is the additional functionality and flexibility it offers. This can be used to advantage when new or improved functionality is needed. However, with any new functionality comes added complexity and potential new or different failure modes. The temptation to implement new functionality that is not really needed should be avoided.

Segmenting the system functions into well defined, simpler subsystems is another approach to reducing overall system complexity. For example, distributing the system functions to a number of individual PLCs versus combining them all in a more complex, general-purpose computer system may simplify the overall design and enhance reliability. The benefits of a simplified design have a compounding effect in reducing implementation, testing, and maintenance efforts.

4.6.4 Examples of Varying Safety Significance and Complexity

The examples provided in this document and in TR-106439 are intended to illustrate a wide spectrum of equipment and systems of varying safety significance and complexity. Corresponding variation in the scope and rigor of the dedication activities can be seen in these examples.

4.7 Determination of Project-Specific Methods and Activities Required

Based on the information collected in the steps above, the specific types of activities that are expected to be required to support evaluation and acceptance of the product(s) should be defined. This early determination of project-specific methods and activities will allow tailoring the project to effectively address project needs, including specific requirements for dedication activities. Note that this early determination of activities and associated level of effort is important in defining the total cost of the project and avoiding surprises. Examples of activities that might be identified include:

- Special testing or other supplemental verification and validation activities (see Section 5.3)
- Survey/design review (see Section 5.4)
- Survey of operating history (see Section 5.6)

For the Example 6.1 LPSI flow indicating controller, plant experience with the device in conjunction with a prior vendor survey minimized special activities required. Example 6.2 involving a device of similar complexity and safety significance required a vendor survey and design review because of the lack of experience with the device and the lack of operating history. The more complex and safety significant systems of Examples 6.4 and 6.5 required significantly more utility/vendor interaction, surveys, reviews and testing.

Selection of the project team members should also be addressed at this stage of the project. The project manager should ensure that the required expertise is available from the team members. Examples of some of the areas of expertise that may be required include:

- Digital systems experience, including hardware and software
- Software engineering, SQA, V&V, configuration management — including familiarity with the IEEE standards on these subjects
- Equipment qualification (including EMI)
- Human factors/HMI

- Licensing
- System engineering, operations, maintenance
- Procurement engineering
- Vendor audit/survey experience

4.8 Cost/Benefit Evaluation

Cost/benefit assessment is a key consideration in determining whether and how to use commercial grade equipment. Substantial effort has been spent attempting to apply cost/benefit analysis to digital upgrade decisions. However, the traditional engineering economics approach to cost/benefit assessment does not apply well to the nuclear plant I&C upgrade cost/benefit evaluations. The benefits of I&C upgrades are known qualitatively, but quantifying these benefits generally has proven difficult. In most cases, the benefits consist of avoided costs, such as a reduced number of plant trips, reduced radiation exposure, and reduced O&M costs. Development of a cost/benefit analysis methodology for digital upgrades, including those that involve use of commercial grade digital equipment, has been addressed as part of the EPRI I&C Initiative.

EPRI TR-101984 and EPRI TR-104963 are two products of the activities directed at this issue. These documents may assist utilities in addressing the elements of cost/benefit considerations. However, in many cases, a decision is made simply on the basis that an added

Avoiding Surprises

At one plant, a new commercial temperature controller was to be installed on a hydrogen analyzer to replace existing switches that were exhibiting poor reliability, and to provide better temperature indication and alarms. Recognizing that the new controller was microprocessor based and included firmware, procedures were invoked to perform a preliminary hazards analysis and define software requirements.

However, in an early look at the device the engineer concluded that the firmware was used only in the initial setup of the controller and would not be used during its normal operation. The controller would function essentially as a switch and thus could be considered a very simple device. (This was incorrect. In fact, the microprocessor and firmware are responsible for sampling and processing the input, comparing temperature to the setpoint, determining the required output, and driving the indication and alarms.) Also, because the vendor had an ISO 9000 program, the engineer concluded that quality of the firmware would be high in any event. (Actually, ISO 9000 certification may demonstrate that there is a written QA program, but it does not necessarily indicate an adequate software development/SQA process is being followed. Also, even if a good process is now in place, this firmware was likely developed long before the program went into effect.)

A procurement specification and request for quote were prepared and sent to several vendors who could perform testing and dedicate the device for this safety application. The request asked only for typical hardware qualification testing, with no requirements for software QA/V&V or EMI testing.

Fortunately, one of the vendors recognized that the controller should be treated as a digital device and would require additional activities to verify adequate software quality and EMI protection, informed the utility procurement engineers, and offered to perform those services as well. However, because the costs of these activities had not been budgeted, the project was stopped as soon as this information was received.

Following the guidance in EPRI TR-106439 and this report will help avoid these kinds of surprises.

capability is needed to meet regulatory requirements, or continued maintenance of an old system is no longer practical. Whatever the situation, cost/benefit considerations will likely be needed for budgeting and may be required to support the decision process in prioritizing plant upgrades.

EPRI TR-104963, "Instrumentation and Control Upgrade Evaluation Methodology," provides guidance on determining the technical and cost-related feasibility of performing an I&C system upgrade. It provides a process for identifying system problems, developing upgrade requirements and a conceptual design, performing a cost/benefit analysis on a variety of system-specific upgrade alternatives, and selecting the most appropriate I&C upgrade alternative. Since the most cost/beneficial solution for a given system is the one with the lowest overall costs over the system life, commercial grade equipment which is normally produced in large quantities and well supported, is often attractive.

A cost/benefit analysis methodology based on a decision analysis and use of “influence diagrams” is provided in EPRI TR-101984, "Application of a Cost-Benefit Analysis Methodology to Nuclear I&C System Upgrades." The methodology addresses data uncertainty, performing sensitivity analyses, and defining the probabilistic distribution of benefits. The benefits of six different types of projects, covering a wide range of I&C upgrades from new hardware component installation to the development of broad guidelines for future I&C upgrades, are examined in this report. Organizations that wish to develop analytical methods for performing cost/benefit analyses may find the information in this report useful.

Two other EPRI reports discuss cost/benefit evaluations for specific applications:

- EPRI TR-104913 addresses cost/benefit evaluations for plant process computer upgrades.
- EPRI TR-106029 addresses cost/benefit evaluations for maintenance planning.

An important cost/benefit aspect of any digital upgrade, whether commercial or developed under a 10 CFR 50 Appendix B, is lifecycle costs. Digital equipment will likely need software maintenance over its lifecycle as well as further upgrades to address obsolescence. Commercial digital products sold in many markets typically are enhanced or replaced with newer versions regularly, to meet competition and take advantage of new technology. This results in a shorter vendor support and spare parts availability period than was the case for older analog equipment. These types of lifecycle costs are difficult to predict, but they should be considered when defining the project.

4.9 Iteration to Define Project and Equipment Options

The flowchart provided in Figure 4-1 loops back to steps in the project definition process, iterating until the project and the alternatives are sufficiently well defined for a decision to be made as to whether to proceed, and with which option, if multiple options are being considered. In most plant modifications, there will be some, and possibly substantial, iteration until all factors and interests involved are satisfactorily addressed.

5

EVALUATION AND ACCEPTANCE

Section 4 described the important issues that should be addressed during the Project Definition stage of an upgrade. This section highlights the evaluation and acceptance activities that occur after the project is defined and the commercial digital equipment to be used has been identified.

5.1 Requirements Definition and Tracking

Studies of software-based systems have concluded that a large fraction of the problems characterized as software errors are more correctly attributed to problems in the requirements specifications, such as errors, omissions, inconsistencies, and ambiguities. The experience of nuclear utilities seems consistent with this result; that is, problems typically involve unexpected behaviors resulting, in part, from ill-defined and inadequately verified requirements.

For any digital upgrade, whether or not a commercial item is involved, the system requirements should be developed, analyzed, and tracked according to some controlled procedure or methodology. One way to do this is described in EPRI TR-108831, which is summarized in section 5.1.1 below. Only after the system-level requirements are defined can the critical characteristics of a potential commercial device be identified and verified.

Figure 5-1 illustrates how the system-level requirements may be allocated to various components and subsystems, and critical characteristics are defined for commercial grade items to meet the requirements. Then, purchase specifications are prepared for the commercial items, along with any services required (e.g., development of application software by a third party under a 10 CFR 50 Appendix B program), and other components purchased from 10 CFR 50 Appendix B qualified suppliers. Several points should be made here:

- The system requirements may be met in a number of different ways, allocating requirements to different components or subsystems as appropriate based on their capabilities.

- This allocation may change as more information is obtained during the design process. For example, the inability to verify a critical characteristic can lead to a different allocation of requirements such that the characteristic is no longer required for the commercial device (the corresponding requirement is shifted to another component in the system).

- A digital upgrade may affect an entire system or it may simply replace a specific component or piece of equipment within a system (e.g., a meter, recorder, controller, etc.). In either case, the system-level requirements must be determined so that the requirements for the commercial component(s) are known. Then, critical characteristics can be identified.

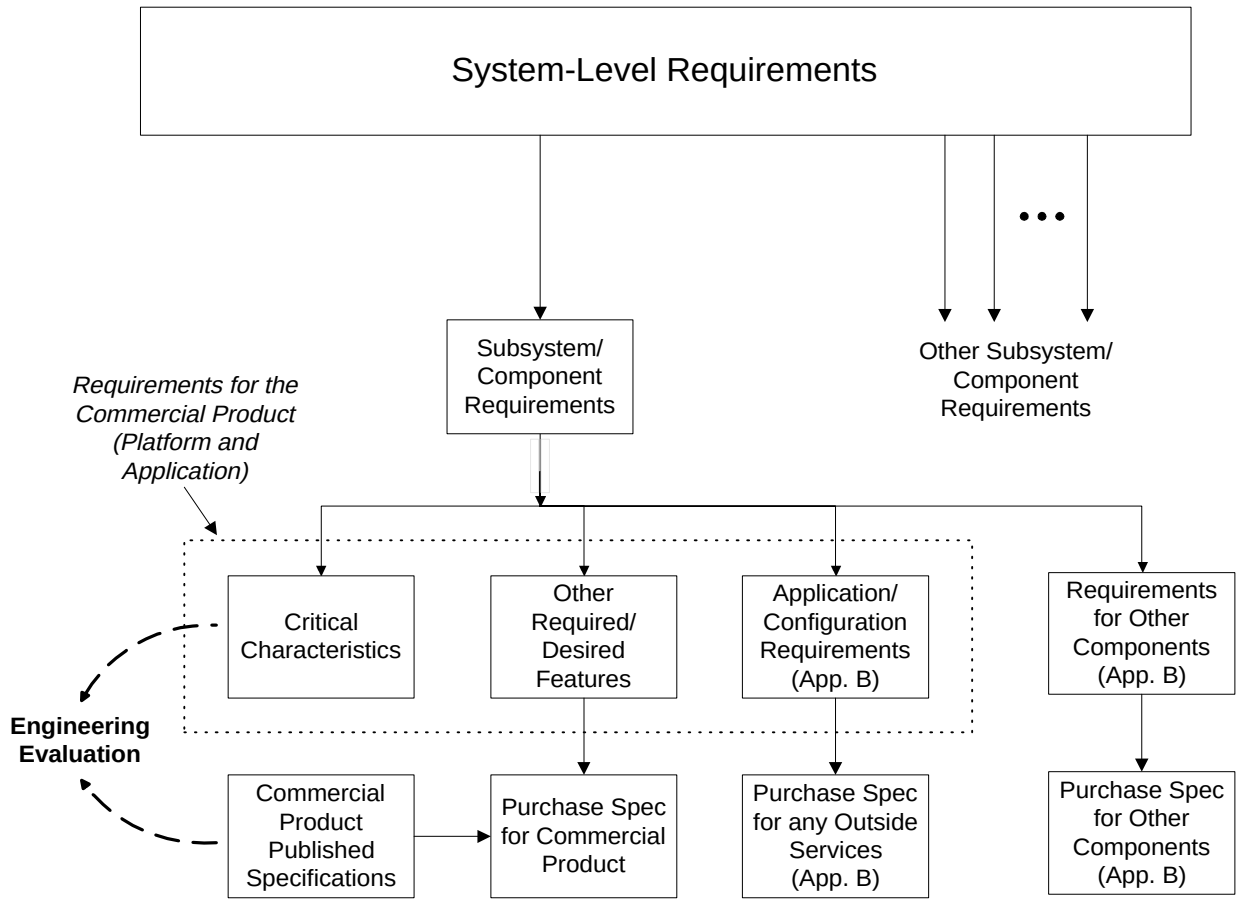


Figure 5-1
Example Breakdown of Requirements from the System Level Down to a Purchase Specification for a Commercial Component

Allocating Requirements to the Commercial Grade Item

This example illustrates the allocation of system requirements to various components and the definition of support critical characteristics. In this case, the allocation of requirements is changed part-way through the project when shortcomings are discovered in the commercial item's ability to meet the original requirements.

An I&C system is about to undergo a digital upgrade, and the system-level requirements have been established (the top-most block in Figure 5-1). One of the requirements is that there shall be no unannounced failures in the system that could affect its proper functioning or readiness to operate. A commercial controller is to be used in the new system. Because the controller is integral to the proper functioning of the system, the system-level requirement regarding unannounced failures is imposed on the controller (Subsystem/Component Requirements block in Figure 5-1).

Initial investigation of the controller indicates that it contains a watchdog timer function that is supposed to detect failures in the device and set diagnostic/error flags accordingly. A requirement for the controller application software is defined, and added to the application software requirements specification, to drive specific outputs in response to these error flags so that they can be sensed and appropriate action taken (e.g., force outputs to a fail-safe condition, or alert the operators if they have sufficient time to act). A critical characteristic is defined for the controller, requiring that the watchdog timer feature be provided sufficient to support the system requirement for no unannounced failures.

When a critical review is performed of the controller design and internal behavior, it is discovered that the watchdog timer does not catch some important controller failure modes. As a result, the designer decides to integrate an external watchdog timer into the design which will provide the required coverage of controller failures. The requirements for this external device are defined such that the system-level requirement will be satisfied (these fall in Requirements for Other Components block on the right side of Figure 5-1). The original requirement for an internal watchdog timer is removed from the list of critical characteristics for the controller. A purchase specification is prepared for the controller based on the published specifications plus some additional plant-specific requirements related to labeling and packaging of the device, spare parts, etc.

Good requirements definition is very important. However, one must also remember that there is no "perfect" set of requirements, and the requirements by themselves do not ensure a successful project. A key area of concern with digital systems is the potential for unforeseen or unexpected failure modes, and as a practical matter it is difficult to write a requirement that will provide complete protection against this. It is important to make the requirements as complete as possible, and to treat as many of the key areas of risk as is practical. But it is also important to recognize what the requirements do **not** do, and to ensure that appropriate effort is applied in the downstream processes and not focused too much on refining the requirements document.

Requirements definition and tracking are discussed further in Sections 5.1.1-5.1.4. Definition of critical characteristics are covered in 5.2. Verification of the characteristics, using the four methods in EPRI NP-5652, are discussed in Sections 5.3-5.6.

5.1.1 Requirements Engineering for Digital Upgrades (EPRI TR-108831)

EPRI report TR-108831 provides guidance on the engineering functions associated with the specification and tracking of requirements for a digital upgrade. These functions include defining, analyzing, and tracking requirements throughout the project life cycle, as shown in the center pane of Figure 3-2. Using this requirements engineering guidebook, a utility engineer should be able to develop a requirements specification for a digital upgrade that will lead to a high quality product while minimizing project risks.

The approach described in TR-108831 is based on three fundamental activities:

- problem analysis
- product description (e.g., the specification)
- requirements analysis

The problem analysis activities are those that occur during the project definition stage. The description of the problem analysis activities in TR-108831 is similar to the discussion in Section 4 of this report, so it will not be repeated here.

The product description section of TR-108831 includes a standard format and content for requirements specifications that include system, hardware, and software issues. Using this generic format helps ensure that all the technical areas are addressed during the requirements development effort.

Requirements analysis transforms the "words" of the specification into an organized, interconnected set of unambiguous requirements. Requirements statements should meet the following criteria:

- Each requirement should define what needs to be done, not how to do it (unless there is a reason to constrain the design)
- Each requirement must be valid, complete, necessary, consistent, unambiguous, feasible, clear, and verifiable

The following three requirements analysis activities are recommended and described in TR-108831:

1. A conceptual design analysis to integrate and clarify the requirements stated in the text
2. A system failure analysis to assure the integrity of the system under abnormal conditions

3. A completeness analysis to ensure a predictable system response for all values and arrival rates of the input variables and trigger events

While a great deal can be done to ensure the adequacy of a specification, digital systems can be much more complex than their analog predecessors, with greater potential for unintended behaviors and subtle failure modes. It is virtually impossible to anticipate all the possible problems and behaviors of the delivered system at the requirements stage. In fact, some of this information cannot be discovered until most of the design work is complete. As a result, proper handling of the conformance checks (i.e., verification that the installed system "conforms" to its specifications) during the design and implementation stages is also necessary to ensure a high quality system.

Conformance checks are quality-related activities that involve interaction between the utility and the vendor, system designer, or system integrator. Conformance checks begin at the requirements stage and continue until the system is placed into service (the O&M stage). The recommended conformance checks (from TR-108831) include:

- Design reviews of the requirements document, the design specification document, the V&V plan and procedures document, and the Users Manual
- Final Design Failure Analysis
- Requirements Traceability
- Factory Acceptance Tests
- Site Acceptance Tests
- Spare parts and qualification tests

5.1.2 Additional Guidance on Defining and Analyzing Requirements

As pointed out in EPRI TR-108831, analysis of the requirements that have been generated is important to ensuring that the requirements are:

- valid
- correct
- complete
- necessary

- consistent
- unambiguous
- feasible
- understandable
- traceable
- verifiable

Iterative Gathering of Requirements

The human-machine interface is a good example of an area where it is difficult to develop a complete set of requirements up-front. In one plant, a PLC was to be installed to provide monitoring and alarm functions for a new accumulator tank being added to the service water system. The basic requirements for the monitoring and alarm functions were straightforward and could be defined relatively easily. However, the requirements for the information display that was to be provided with the unit were more difficult. Here, input was needed from plant operations and maintenance personnel to determine how the display would be used, the information needed, appropriate terminology, grouping of alarms, etc. The commercial device's limitations in terms of the ability to customize the display through programming greatly complicated the situation. In this case, the final requirements could be determined only after some initial programming was done to demonstrate the display to the appropriate personnel, sufficiently engaging their attention and demonstrating the capabilities and constraints of the device.

Ensuring completeness of the requirements requires getting attention and input from all the key stakeholders in the project, including engineering, operations, maintenance, and perhaps others. Again, this inevitably requires some iteration that should be planned for when scheduling the activity.

5.1.3 Guidance on Preparing Procurement Specifications

For commercial equipment, the procurement specification often is based primarily on the vendor's published specifications (see Figure 5-1). The dedicator ensures that the commercial item will meet the requirements of the application. This is fundamental to the concept of buying commercial "off-the-shelf" equipment—the equipment is purchased based on the vendor's specifications with little or no imposition of special, nuclear-specific requirements on the commercial supplier.

If screening of the vendors is done as part of selecting the vendor, then there may be items from the screening criteria that should be reflected in the procurement specification (e.g., specifying that the QA and configuration control programs described by the supplier as part of the screening process be used in the production of the unit to be supplied). If a vendor survey is done prior to the purchase, then the specification should request a Certificate of Conformance to the program that was examined in the survey. The survey may also identify other items (e.g., options that should be specified to ensure the required critical characteristics will be met).

It is important not to over-specify the equipment. Specification requirements that clearly will not or cannot be met by the supplier simply reduce the credibility and value of the specification. Remember that the vendor is most likely to control those characteristics that are published in a product specification. Specifying other desired

characteristics or parameters that are outside the normal published specs may not in itself ensure that these characteristics are controlled — special effort may be required to verify these.

As discussed above, if standards are referenced in the specification, the references should be specific and consistent with the actual practices followed by the vendor. Blanket reference to a nuclear standard that is not even familiar to the supplier is not useful and can cause confusion and misunderstandings between supplier and customer.

The procurement specification should include requirements for any needed support of the dedication. For example, if a survey and a Critical Digital Review (CDR) are to be performed and the vendor will be paid for supporting the review, then the specific needs for support should be included in the specification requirements (e.g., x days of time from knowledgeable engineering staff to support the design review). Also, the specification should address any other requirements for access to information (e.g., access to source code), requirements for problem reporting and software updates (e.g., subscription to error report service and notification of upgrades/fixes).

It's Specified, But is it Controlled?

Suppose that the published specifications for a controller indicate the device is unaffected by EMI for radiated field strengths that are below X volts/meter up to a frequency of F. It turns out that the requirements for my application call for EMI immunity up to 1.2X volts/meter at frequencies up to 2F. To check this, I obtain a unit from the vendor and run my own EMI laboratory testing. The tests show that the device will meet the more stringent requirements of my application, though without much margin. When I get ready to purchase the units I need for the plant, I include in my purchase specification a requirement to meet the higher EMI susceptibility limits.

But what is the vendor supposed to do with that requirement? The test was paid for and run by the utility. The vendor's testing has demonstrated only that the published specification limits are met. Furthermore, as this product is manufactured over time, the vendor is confident based on his own controls that each unit produced will meet the published specs. But will he take steps to ensure that the more stringent requirements of this one application are met?

That seems doubtful. In any event, I should not count on the specification requirement to ensure it. For each procurement, I may need to re-run the EMI laboratory testing to verify continued compliance. Including the higher EMI limits in the procurement specification is probably meaningless, and could lead to confusion on the part of the vendor or false expectations on the part of the customer.

5.1.4 Requirements Traceability

Requirements traceability refers to the tracing of requirements through the design (features or modules intended to address each requirement) and through testing (tests intended to address each requirement). Typically a Requirements Traceability Matrix (RTM) is used to document the traceability.

A requirements traceability matrix can be used at different levels and in different parts of a digital upgrade project. For example, an RTM may be developed to trace application software requirements through the design and testing of the application

software (e.g., PLC ladder logic). Also, when reviewing a vendor's software development process (e.g., as part of a commercial grade vendor survey), requirements traceability is an item that should be reviewed—did the vendor develop an RTM? If so, was it complete? If the vendor's process did not include or document traceability, it can be checked and documented to some degree during the assessment of the software, by selecting items in the software requirements specification (assuming one exists) and tracing them through the software design, implementation and verification. Note that a thread audit is in part a traceability analysis for a sample of the requirements (see Section 5.4 and Appendix A).

EPRI TR-108831 provides additional guidance on requirements traceability. Remember that the RTM should be a **tool** and not just a document that is prepared. If you prepare it, **use** it to help make sure that all requirements are appropriately addressed in the design and are verified. For application software, the basic requirement is that there be traceability of the requirements through the design and verification. An RTM can help ensure such traceability is present, or make clear where it is not. Note that in some cases a very simple RTM may be used with two columns, the leftmost being the requirement (e.g., a paragraph from a requirements document) and the right column simply giving a brief description of how this was verified. For more complex projects, it may be helpful for the RTM to list the requirements paragraph, a reference to the design documents indicating where the requirement is covered in the design, a test plan or procedure reference indicating which test step checks the requirement, and a user's guide reference indicating where it is reflected in the user documentation (if appropriate). A simple database may be warranted to help manage the RTM for a large project with many requirements and verification activities.

5.2 Definition of Critical Characteristics and Formulation of an Acceptance Strategy

Readers should be familiar with the basic process described in NP-5652 for definition and verification of critical characteristics using one or more of four acceptance methods. EPRI TR-106439 describes how to apply this process for commercial digital equipment.

5.2.1 Differences With Digital - The "Digital Delta"

EPRI TR-106439 describes how the dedication process differs for digital equipment as compared to other types of equipment that have routinely been dedicated in the past. The primary differences encountered when dedicating digital equipment can be summarized as follows:

- Digital equipment introduces new complexities or subtleties to verification of some of the same critical characteristics that always have applied to I&C equipment. For example, checking response time of an analog instrument is relatively straight-forward and can be verified by a simple test—apply an input and time the output response. Given an understanding of the principles of operation of the circuitry, an engineer can be confident that this test will suffice to verify response time. However, with a digital instrument a test giving acceptable results under one set of conditions may not ensure that acceptable time response will be obtained under some other conditions, because the time to respond includes delays associated with internal processing of the inputs and may be affected by behavior of other inputs, servicing of other tasks, etc. More extensive testing, use of operating history, and/or examination of the internal data processing architecture may be required to verify the time response characteristic.

- With digital equipment, dependability of the device is a much bigger issue than with analog. In a system based on analog electronics, non-programmable solid state logic, or relays, the behavior of a system output is determined by the state of the inputs and, typically, a relatively straightforward signal path through the system. With a computer- or microprocessor-based system, the output behavior also depends on software that processes the inputs and, based on these inputs and the states of internal memories, determines the outputs. The number and complexity of the possible paths a signal may take through this software processing are much greater. There are many more possibilities for errors, or abnormal conditions or events (e.g., see IEEE 7-4.3.2) to disrupt or corrupt the signal processing and the outputs. Also, the potential consequences of these errors or events can be more severe, bizarre, and difficult to predict. Unintended functions may occur, and new failure modes may be present. "Black box" testing alone is not sufficient to verify dependability of digital equipment. As a result, additional critical characteristics will be needed beyond those normally specified for an analog device. For example, as described in TR-106439, built-in quality of the software is a key characteristic that must be verified for commercial digital equipment.

These are important differences. However, the same basic process and the same methods can be applied in dedicating commercial digital equipment. TR-106439 provides the framework showing how this can be done. The following paragraphs provide some additional guidance.

Examples of the Digital Delta

Appendix A cites some examples that illustrate the digital delta and problems that can be caused when it is not understood. In one case, a PLC is installed to replace solid state logic in a safety system. With the old system, certain output states that were considered "invalid," and would have undesired consequences, could not occur unless there was a failure or malfunction of the system. However, the system logic includes internal feedback that can result in different behavior when processed sequentially by a digital device. With the PLC implementation, which relies on a scanning process to sense the inputs and then process the logic, intermediate unstable output states can occur as the PLC responds to changes in the inputs and takes more than one scan cycle to completely process the logic. The Appendix describes how a problem could be created when this situation is combined with a fault tolerant scheme intended to detect and respond to invalid output states. See Appendix A for this and other examples of the digital delta.

The examples in TR-106439 and in Section 6 of this document provide a good source of "how-to" information for selecting critical characteristics and verification methods. They provide a number of specific dedication examples covering a wide range of complexity and safety significance. These examples illustrate the selection of critical characteristics for different types of equipment, including the "dependability" characteristics, and choice of specific verification methods that could be used for each. Remember that these are examples only; the lists of critical characteristics are not intended to be all-inclusive.

All critical characteristics must be verified in order to accept an item. Therefore, it is important to limit the list of critical characteristics to those that are required, and eliminate any that are not. For each characteristic, ask yourself what would happen if that particular characteristic could not be verified, for one reason or another. Would another characteristic (once verified) in fact cover what was intended by this one? If the characteristic cannot be verified, would the item still be acceptable if established utility procedures and the guidance in EPRI NP-5652 and NP-6406, and the 10 CFR 21 regulation are applied? If so, the characteristic should be eliminated from the list of *critical characteristics for acceptance*.

Some characteristics may be required for reasons unrelated to the device's safety function. Inability to verify one or more of these may be reason to reject the item. However, if these characteristics are not strictly required for dedication of the item, then it is best to keep them off the list of critical characteristics and treat them separately.

5.2.2 Selecting Verification Methods for Specific Characteristics

Although EPRI NP-5652 allows for any one of four methods to be used in verifying the critical characteristics and accepting a commercial grade item, typically a combination of two or more methods is required for digital equipment. Table 4-1 in EPRI TR-106439 provides examples of methods that may be applied in verifying some of the key critical characteristics for digital equipment. These are not exhaustive lists, but are intended to illustrate the types of verification methods that might be used. Remember that there is no one set of verification methods that must be used to verify any particular characteristic. The most appropriate methods to use must be determined for each dedication, and will depend on a number of factors, including:

- The safety significance and complexity of the equipment — see Sections 4.4 and 4.6 for discussion of grading based on safety significance and complexity
- The strength of the vendor's process and documentation — this will determine how much credit can be taken for these in demonstrating adequate built-in quality, for example
- The performance record of the equipment and the vendor — determining the degree to which operating history can contribute to the verification of critical characteristics.

5.2.3 Expertise Required

People who have experience in design, procurement, and vendor audits or surveys should have input into the definition of critical characteristics and determination of appropriate verification methods. Also, digital systems expertise typically will be required. The need to apply special expertise in dedication is not new — utilities have always used "technical specialists" to assist in identifying and verifying critical characteristics when required (e.g., involving a metallurgist when special material properties are at issue). Digital systems specialists can be used in the same way, drawing from within the utility's own pool of talent or from the outside if necessary. Many utilities are building up this type of expertise in their engineering departments, or using team approaches that draw on expertise available from other departments to supplement I&C and procurement engineers on a project.

5.3 Testing

Testing falls under acceptance Method 1 in NP-5652 and is the most commonly used method for commercial grade item dedication. Functional and performance testing is used as part of accepting virtually all I&C equipment. However, for digital equipment testing by itself is seldom sufficient for acceptance. Typically, inspection and testing under Method 1 are supplemented by a commercial grade vendor survey (Method 2 —

see Section 5.4) and a review of the equipment's performance record or operating history (Method 4 — see Section 5.6). Also, under Method 1, special tests designed to address specific digital issues may be required in addition to typical "black box" functional and performance testing.

Additional guidance on testing is provided in the following paragraphs. This guidance focuses on digital-specific issues. Other existing standards and guidelines should be consulted for guidance on testing in other areas (e.g., seismic, environmental qualification, EMI emission and susceptibility testing).

5.3.1 Types of Testing

It is important to focus testing in areas of highest risk or on the most critical parts of the system. This is consistent with the graded approach recommended in TR-106439 and discussed in more detail in Sections 4.4 and 4.6 of this document. Critical, high-risk areas are determined based on safety significance and complexity. This concept applies to non-safety systems as well, but using plant economic risk, personnel risk, etc., in addition to plant safety.

The vendor's testing should be reviewed and the need for any special or supplemental testing defined. Once the vendor testing has been reviewed, a good approach is to follow a two-stage process to develop a test plan, and then specific test procedures. The test plan can identify what specific types of tests will be covered in the different test programs that will occur, e.g., Factory Acceptance Testing (FAT), Site Acceptance Testing (SAT), post-installation or startup testing, and any special tests that need to be performed. (Note: The SAT may be completed as part of post-installation testing if separate acceptance tests are not required prior to the installation.)

If an entire system is being purchased as opposed to a single instrument or device (as in Examples 6.4 and 6.5 which involve monitoring and control systems making use of a number of components including commercial digital products), more than one FAT may be involved. There may be a FAT performed by the supplier of the commercial product (e.g., a PLC), and then a system-level FAT performed by the integrator for the overall system. The same applies to the SAT. One SAT may be performed as part of accepting the commercial item, and a system-level SAT performed for the system as a whole. The test plans should spell out what tests will be performed, and of course the dedication package must document which specific tests are used to verify critical characteristics of the commercial grade item.

In FAT and SAT testing, actual plant conditions should be replicated to the greatest degree practical. Characteristics of the inputs and outputs (including wiring configurations), power supply, and other conditions should be as close as possible to the actual expected conditions. Post-installation tests will serve as final integration testing in the actual plant configuration, but the earlier tests should be designed to minimize the chance of problems occurring in the post-installation phase.

Factory Acceptance Testing should go beyond simple performance tests based on the functional requirements. Tests of behavior under expected abnormal conditions and failure modes should be performed (e.g., response to loss and restoration of power, loss of signal, etc.). Also, "stress" or "challenge" testing is important. Tests should be devised that examine behavior under conditions of heavy communication loading, processor loading, and other high-stress conditions. Also, for a complex system, free-form testing of random input combinations and sequences, actuation of controls or operator inputs, and other informal testing can be very helpful in checking robustness of the system and finding unexpected behavior before it is found in the plant.

Appendix B of NUREG/CR-6421 provides detailed information and guidance on different types of software testing, which techniques are most suitable for verifying different software qualities or attributes of interest, who should conduct testing and independence of testers, prerequisites for testing, and guidance on selecting a test strategy. It includes discussion of stress or challenge testing, which is particularly important in ensuring dependability of digital equipment.

5.3.2 Use of Test Plans and Digital System Models

For most digital equipment, no test program can provide complete assurance that all conditions have been covered and all potential problems have been found. Typically, testing must be coupled with an understanding of the internal system architecture, signal paths, task management and prioritization, timing constraints, etc. The French have recognized this in developing their test plans for qualifying control systems for the next generation of French nuclear plants. The utility, EDF, is using an approach that couples testing with system "models" that describe how the control system is expected to operate. For a simple system, the model may simply be an analysis or description of the architecture and performance of the system. For more complex systems (e.g., distributed control systems), computer models are used. In either event, the purpose is to gain a sufficient understanding of the system to be able to interpret the test results and know how far they go in providing the needed assurance.

Appendix B provides some sample test plans developed by EDF for control system qualification. The plans cover digital system signal paths and timing issues (e.g., transit time of information through the system). They describe:

- The control system architecture for the system being tested
- Test requirements (e.g., enumeration of the various signal paths that must be tested)
- System modeling to determine the internal "technical functions" of the system that support the performance being tested (e.g., breaking down functions such as scanning, filtering, processing, transmission, etc.)

- Conditions that are expected to influence performance during the tests, and thus must be considered in the test program (e.g., environmental conditions, power supply characteristics, other tasks being processed, etc.)
- Organization of the tests into logical sets of sub-tests, with repetitions defined
- Test configuration, test measures and test equipment requirements
- Plan for analysis of the results, comparison with the models, and expected use of the test results.

These sample plans may serve as models for development of test plans and procedures to support dedication of commercial equipment in U.S. plants.

5.4 Surveys and Design Reviews

This section relates to Method 2 in NP-5652, Commercial Grade Survey. In addition to surveys, it discusses use of design reviews and methods for obtaining information on the internal operation of digital equipment that is often necessary in order to verify the critical characteristics associated with dependability and failure modes. Such design reviews often can be combined or coordinated with a commercial grade vendor survey.

5.4.1 Commercial Grade Surveys and Design Reviews for Digital Equipment

For many commercial grade items dedicated for nuclear applications, the critical characteristics of the item are verified primarily through inspection and testing. For example, relatively simple hardware items like mechanical parts (e.g., fasteners) and electrical equipment (e.g., conventional circuit breakers) can be tested to verify, with a high degree of confidence, their performance characteristics. Engineers can inspect and review the hardware designs, documentation, and physical equipment and verify that the items will meet the applicable requirements and will operate dependably, without reviewing in detail the specific processes or methods used by the vendor in designing and developing the equipment.

For digital equipment, a new dimension is added due to the reliance on software for proper operation of the equipment. It is well established that the dependability of software, of the size and complexity used in most I&C equipment, cannot be established by inspection and testing alone. The process used to develop the software is a very important factor in ensuring that the final product will meet its requirements under all conditions that may be encountered in service. As a result, a survey of the vendor's software development and quality assurance practices is often required. It serves to verify critical characteristics related to built-in quality and dependability, which are especially important for software.

In addition, for equipment that is critical to plant operation and/or safety and thus requires very high dependability, gaining knowledge of the vendor's software development process still may not provide all the information and assurance needed to accept the equipment. There are many standards, procedures and methods for developing software, and a survey team can check the vendor's processes against these standards. However, none has been shown to provide, by itself, the high degree of assurance required for critical software, particularly when one considers abnormal conditions and events (see IEEE 7-4.3.2) and unusual failure conditions that can occur with digital systems.

By its nature, digital equipment has the potential to exhibit obscure behavior and unique failure modes. To assess the potential risk associated with such behavior, it is typically necessary to gain an understanding of the digital system's underlying design, software architecture, and real-time data processing, and to perform a failure or hazard analysis at some level for the equipment. Therefore, in addition to examining the vendor's quality assurance and software development procedures, a commercial grade survey for digital equipment often includes or is supplemented by a critical design review and failure analysis. These kinds of reviews and analyses can be incorporated directly into the survey plan, for example.

Appendix A describes one method that has been used successfully in performing a critical review for digital equipment. Referred to as a Critical Digital Review (CDR), this method has been applied both for commercial equipment and equipment developed under a 10 CFR 50 Appendix B program. It is a focused, technical review of the digital product and the vendor, performed primarily at the vendor's facility. The CDR includes:

- A "system orientation" in which the review team gains an overview of the digital system architecture
- A "process orientation" in which the team determines how the vendor develops, supports and maintains its products
- A "thread analysis" that includes detailed, systematic tracing of specific functions through the vendor's product and processes
- A "risk analysis" that combines a qualitative fault tree analysis and a qualitative failure modes and effects analysis to assess the risk associated with potential undesirable behavior of the product.

A Critical Digital Review or other form of design review typically provides information that is needed to verify some of the critical characteristics for digital equipment. It may be performed separately, but it is often combined with a commercial grade vendor survey. Performing the two in a single visit may be the most efficient approach because of the overlap between the two reviews and the fact that the vendor may find it less intrusive to host one rather than two visits. However, it is important that each review

has the appropriate personnel to coordinate and carry out the needed activities. Appendix A includes a discussion of the functions performed by personnel needed for a CDR and how these may or may not overlap with the people who typically perform vendor surveys and audits.

5.4.2 Use of Industry Standards and Product Certifications

Many I&C equipment vendors are pursuing certification to various industry or international standards. Although, at present, none of these serves as a direct substitute for 10 CFR 50 Appendix B qualification of a vendor, availability of such certifications may reduce the effort required for a vendor survey in support of dedication.

Certification to the ISO 9000 standard is a step in that direction. However, experience has shown that there is significant variability in the quality of vendors and vendor processes actually followed among organizations that are ISO 9000 certified. It is important not to simply accept the fact that the vendor has been certified and take credit for this in checking the vendor's quality assurance program. First, the equipment to be procured (and its software) may have been developed long before the QA program was certified (and probably upgraded) to ISO 9000 status. Also, the practices actually followed by the vendor may not meet the utility's requirements in spite of the programmatic certification.

There are other certifications that a vendor may undergo. For example, the TÜV certification authority in Germany certifies programmable electronic system (PES) products for use in safety systems. The report of the certification in some cases provides a relatively detailed description of the system, its internal architecture, results of inspections and analyses including failure modes and effects analysis, and extensive testing. However, it still must be determined what was actually done in the reviews to support certification, what criteria were used, and how these stack up against the criteria for dedication.

Also, it is important to note that TÜV certification may be granted with certain restrictions or "provisos." The purchaser should check the certification report to gain an understanding of these. This is important for two reasons: 1) it may affect the degree to which the certification can help provide verification of some critical characteristics, and 2) it may provide information useful for the application of the equipment (e.g., do's and don'ts that should be followed to ensure dependability of the application).

5.4.3 Holding Down the Costs of Surveys and Design Reviews

It makes good economic sense to pursue methods for sharing or reducing costs associated with surveys and design reviews. For example:

- Partnering with suppliers
- Utility teaming, sharing the results and reducing each utility's costs
- Pre-screening to avoid wasted efforts (this is discussed in Section 4.5)
- Use of previous NUPIC surveys; as in the case of 10 CFR 50 Appendix B audits of vendors, NUPIC also keeps records of commercial grade surveys performed by NUPIC utility survey teams.

5.5 Source Verification

This is the third acceptance method outlined in EPRI NP-5652. It refers to a situation in which the purchaser or dedicator witnesses specific activities as they take place at the supplier's facility, to verify that the supplier adequately controls the critical characteristics of the item. Of the four methods, this one generally has the least applicability to digital equipment, as the built-in software used in a commercial device has been developed well before the order is placed for the equipment. However, this method may still be used in some situations. For example, source verification might be used to:

- Monitor the installation or loading of software or firmware into the specific units being supplied. This might be done to provide additional assurance that the correct version is installed and appropriate error-checking done to ensure there were no errors in the download or burn-in process.

- Monitor or oversee quality control of software modifications. This could provide added assurance that software modifications requested by the purchaser are made in accordance with requirements for configuration control, and verification and validation of the changes.

5.6 Use of Operating History

This topic relates to the fourth method outlined in EPRI NP-5652 for verifying critical characteristics, referred to as Supplier/Item Performance Record. Use of the performance record or operating history to demonstrate adequacy of commercial digital equipment is very important in achieving a net cost savings associated with use of this equipment. One of the main advantages cited for commercial digital equipment is that its wide application in other industries can, if successful and relevant to the nuclear application, be used to help demonstrate that the equipment will perform satisfactorily. It is generally accepted that **operating history alone is not sufficient to demonstrate adequacy of a device that contains software. Other methods typically must be used** to provide reasonable assurance the device will perform satisfactorily in nuclear safety service. However, if we do not take advantage of operating experience gained by widely-used commercial equipment, we will not reap the advantages it offers, and the

effort to dedicate the equipment will not be largely different from that required to develop and qualify a device under 10 CFR 50 Appendix B.

Figure 5-2 illustrates a process for obtaining and evaluating operating history data. Note, however, that this need not be a separate activity. The operating history review should be driven by the dedication process -- verification of specific critical characteristics. But it is important to approach the use of operating history in a methodical way. The figure shows some prerequisite information that is needed in order to efficiently gather and evaluate operating history data. Apply this process when evaluating operating history for verification of specific critical characteristics, tailoring it accordingly. The process also can be used for a general review of operating history, for example, for building confidence in equipment that will be used in a critical non-safety application.

The following paragraphs below provide additional guidance and examples.

5.6.1 Scope of Operating History Review

The review of operating history should be focused on those areas where the history data is needed to support verification of the critical characteristics. For example, if testing has provided verification of most of the characteristics related to functionality of the device, but is not considered to provide sufficient verification of the adequacy of self-diagnostic features in covering the device's hardware failure modes, operating history may be needed to complete the verification of self-diagnostics coverage. In this case, the review might focus on obtaining information regarding any failure modes discovered in service that were not detected by the self-diagnostics. In the evaluation, the amount of operating experience may be compared to the requirements for availability and reliability of the device in its intended application to determine whether the experience data is sufficient to indicate that the probability of undetected failures is acceptable. Of course, the relevance of the operating history must be established to ensure that factors such as the configuration of the device, the environment (temperature, vibration, etc.) and the way in which it is operated are sufficiently similar to the intended application that the experience data is valid.

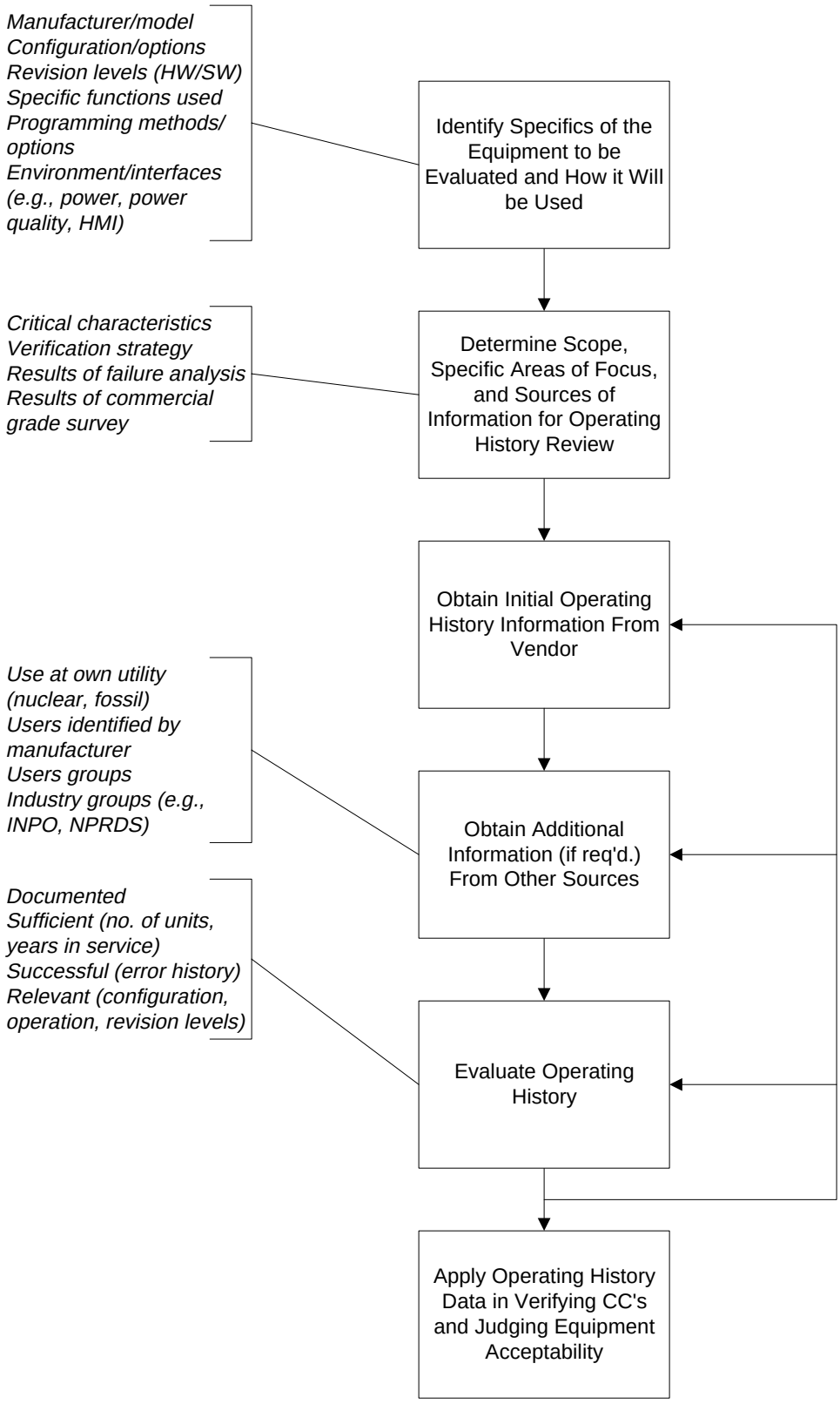


Figure 5-2 Review of Operating History

Note that even if operating history is not formally credited in verifying the critical characteristics, it is still a good idea to obtain information on others' experience with the device. At a minimum, the vendor should be queried about field experience with the product. If there have been any critical problems reported from field applications, you should make sure that you have unearthed these through your questions to the vendor on operating history.

5.6.2 Sources of Operating History

Operating history data may be gained from a number of different sources. The applicability of the data and the difficulty in obtaining it can differ greatly depending on the source that is used.

Various sources of operating history data include the following.

Vendor

The manufacturer or supplier of the equipment is the first and most obvious source of data. The vendor should be asked to supply information on operating history of the product being evaluated. Try to reach the department or individuals who have the most direct knowledge of the operating and repair history for the device -- for example, technical support, field service, repair, and/or quality assurance personnel. Before making use of the vendor data, make sure you understand what data are actually recorded and how this is decided. Some of the problem history may not be formally recorded by the vendor if the problems are considered minor, or the fixes can be made quickly and easily.

Use Within Your Own Utility

Experience data from applications within your own utility, if any, can be a good source of data. Although the applications may be limited in number, the information is likely to be easier to get and validate, and its relevance can be judged more easily than data from other users or other industries. Find out whether the device has been used in nuclear plant applications (e.g., nonsafety-related applications) or in fossil plant applications.

Other Users

Try to obtain information from the vendor on customers who have gained experience with the product. Based on what information is available on how the product is being used and how many units are in service, choose the users who are likely to provide the most relevant information and have the greatest amount of experience with the equipment. Contact those users and try to reach someone who has direct experience

with the operating and maintenance history of the device (e.g., a plant engineer versus headquarters office, plant maintenance engineers/technicians).

User Groups, Industry Reports

For some commercial products or product lines there are formal or informal user groups that share information and experience with the product. Ask the vendor to identify any such groups, and ask users if they are aware of any such information-sharing organizations. Some information may be available through Internet news groups or mailing lists. Search the Internet for information on experience with the product, and post questions on applicable news groups or mailing lists.

Check nuclear industry sources for any experience data with the product. For example:

- INPO's NPRDS and EPICS systems
- NUSMG Bulletins
- Notices issued under 10 CFR Part 21
- NRC Information Notices

Caution should be exercised when using the data from these sources. They may not be very complete, so an absence of problems reported via one of these sources does not necessarily demonstrate that none occurred. Also, the data obtained may not be as reliable as data you may collect directly from users of the equipment.

5.6.3 Questions to Ask

The specific questions that should be asked when soliciting operating history data depend on the source being queried, the type of equipment and the application in which it will be used, the critical characteristics and which ones are most in question or are most critical to the dedication based on the design and failure analysis, and the extent to which operating history is needed to complete the verification of the critical characteristics (i.e., to what extent other methods are providing verification). A sample list of questions is provided below, organized according to the source of the data.

Questions for the Vendor

When was this product first placed on the market?

How many units have been sold?

Approximately how many unit-years of operation have occurred with this device, based at least on the number sold and when?

Do you have specific records of which revision levels of hardware and software were supplied to each customer?

How many revisions have there been? How do you decide when a change warrants a new revision level? What types of changes are made without going to a new revision level?

How do you classify reported errors with regard to their severity or consequences?

What has been the history of errors, particularly critical or severe errors (based on the intended application) for the specific model being considered?

What process do you follow for error tracking, reporting, and customer notification? Who is notified and how? Are open error reports available for customer review?

Do you offer subscription services for reporting errors and fixes? What types of errors or customer feedback reports are covered by this?

Questions for Users

Extent of Experience

How many units are operating in this application?

How long have they been operating (average)?

Relevance

What are the specific model numbers?

What are the revision levels of the hardware and firmware?

What equipment configuration (number and type of modules, interconnection of modules, etc.)?

Overall system configuration: Part of a redundant system? Effects of failures on system?

Which software tool and what revision level was used to develop the application program, configure and load the unit?

What is the basic functionality for this application?

Software components/blocks used: which ones (or ask about specific ones to be used)?

Size and complexity: How many inputs and outputs? What/how many functions performed? How many segments or networks of logic, how many rungs or function blocks implemented, etc.? What scan time, and what fraction of scan time used to process the application? What is complexity of operator displays/HMI?

What is the environment in which the equipment is used? Ambient conditions: temperature, humidity, EMI/RFI, vibration, etc. Power conditions: voltage range, quality (in general, or based on similarity of electrical system and loads).

Operational environment: How used by operators? How often used? How critical to operations? Consequences of failure, and typical actions taken as a result (e.g., reset system, pull and replace, shut down). Level of skills and training of operators and technicians?

Time response issues: What response time required? How challenging is application in terms of speed? What are the most demanding conditions, and how often do they occur?

Accuracy requirements?

What diagnostic and self-test functions are implemented? Which ones are not?

Success of Operating Experience

Track failure rates and/or repair/replacement rates?

Perform root cause or other (formal/informal) evaluation of causes of failures?

Number of failures experienced, and how rate of failure has changed over time?

How were failures detected? What was the nature of any failure(s) not detected by internal self-checks? What is the potential that failures could go undetected, and thus unreported (e.g., due to periodic reset)?

What corrective actions were taken after failures?

How stable has firmware been in recent history?

Documentation

Are installed revision levels documented? Are changes to hardware or software while in service documented?

Are failures in service documented? Are repairs/replacements documented?

5.6.4 Evaluating Operating History Data

EPRI TR-106439 states that operating history should be evaluated with respect to:

- The degree to which it is documented (written records, history traceable to specific model/revision, etc.)
- The extent of the operating history (e.g., number of units and number of years in service)
- How successful the experience has been (number of reported errors or problems encountered, severity of errors, trend in error rate and severity)
- Degree of relevance of the operating experience (same or similar hardware/software configuration, functions used, how the equipment is operated, etc.)

In order to take credit for operating history, it will typically be necessary to address all four of these areas. For example, operating history that has been quite successful in other industries may not be meaningful if you cannot show the relevance of the history to the planned nuclear plant application. Also, operating history that is believed to be relevant and successful but which is not documented other than in verbal statements from the vendor probably could not be credited in a dedication.

The extent to which each of these four aspects of operating history must be researched, and the degree to which they must be demonstrated and documented, will vary depending on the amount of reliance placed on the operating history in verifying the critical characteristics. For example, if operating history is the primary or only basis on which to judge that a particular characteristic is verified, then this places significant emphasis on the history data. More typically, however, operating history is used as one of a combination of methods for verifying critical characteristics and thus it represents only one factor in forming an overall judgment of adequacy.

Note that relevance of the history data is particularly important, and it can be difficult to establish. In particular, it should be emphasized that relevance must be addressed when the questions are asked, and the data is collected. Relevance of the data typically cannot be established after the fact during the evaluation, if the right questions were not asked originally.

5.7 Case Study

This case study consists of an anecdote involving a digital feed pump speed governor upgrade. It makes some key points as indicated below.

Key points illustrated:

- Subtle differences in your specific application of a digital device can cause problems that have not been seen by other users whose extensive, successful operating history is reviewed during the evaluation (unusual use of proportional-plus-integral control module in a proportional-only mode). Also, differences in operating system version can make a difference in failure potential of your application as compared to other users' experience (newer operating system version conflicted with old programming of proportional-plus-integral module).

- The use of diverse backups or mitigation strategies can be a valid approach for addressing potential software failure modes, and in some cases may be more cost effective than performing extensive software/system reviews.

Description of change. New digital governors were installed for the three main turbine-driven feedwater pumps in a BWR. The new governors replaced older, mechanical/hydraulic governors. The governors control steam flow to the turbines to regulate pump speed and thereby control feedwater flow. The governors are not safety-related equipment, but clearly are very important to plant operation and safety due to their ability to affect reactor feedwater flow.

Failure analysis. A system-level failure analysis was performed to examine the effects of governor failures on the plant. Failure of any one governor in a direction to reduce feedwater flow was determined not to be significant, because any two pumps can deliver nearly full rated flow. Failure of up to two pump governors in a direction to increase flow also was determined to have acceptable consequences. Failure of all three governors (e.g., a common mode software failure) in a mode that produces pump speed at just below the mechanical overspeed trip setpoint could produce a total flow rate which was in excess of the maximum flow rate analyzed. Thus this type of failure was determined to be the worst case failure, and represented a previously unanalyzed failure mode for the system.

Operating history review. In selecting the new digital governor, the utility chose a mature product (in service for 10 years) from an established vendor. A customer reference list was obtained from the vendor, indicating sites where the governor was used and how many units were in service at those sites. The utility contacted several sites by telephone, and a team of utility personnel visited one of the commercial sites where the governor was in use on a similarly rated pump. Also, a fossil plant owned by the same utility had recently made a similar upgrade using the same digital governor, and this site also was visited. Information from the fossil plant visit uncovered a potential problem with the governor oil system based on their experience, and this led to a change in the modification design (unrelated to the digital aspects of the change). Telephone calls also were made to several nuclear plants where the digital governor was used.

Digital system/software evaluation. The vendor developed the "application software" in accordance with utility specifications. The utility performed a detailed review of this software prior to its leaving the factory, and this resulted in some changes to the software. The software for a sampling of the built-in "function blocks" also was reviewed, but no detailed review was performed for the base operating system software. Testing was performed to verify performance of the governor.

Resolution of common mode software failure. The utility decided to address the worst-case failure mode by installing a separate, independent speed sensing relay on each of the three pumps to sense a high speed condition. Contacts from all three relays were wired in series to a resistor to shunt control current away from the turbine governor valve actuators. A high speed condition on all three pumps simultaneously will cause all three governor valves to partially close and effectively limit pump output

to below the maximum flow rate analyzed. This diverse function effectively bounds the failure modes of the governors from a system standpoint, and prevents the worst-case failure from causing an unacceptably high reactor feedwater flow. This approach was considered more cost effective than performing additional reviews and verifications of the governor software to try to demonstrate that the common mode software failure of concern would not be likely to occur during the plant life.

Problem encountered in service. A digital system related problem was discovered while attempting to tune the new governors during startup. Although the governor control module was set for proportional-only control, the reaction of the governor was indicative of proportional-plus-integral (PI) control. A PI control module is used in this application, but an input to this block had been set to force proportional-only (P-only) mode. This was a shortcut method that avoided having to switch to a proportional-only control module that would require no special settings. The application software is burned into ROM. When the unit is started up, the program is transferred to an EEPROM. Unfortunately, the EEPROM was getting corrupted during the tuning exercise. This was caused by a conflict between the operating system software (recently upgraded) and the original PI module software. Each used the same variable name for two different purposes. The utility was unaware that the operating system version had changed for the units they purchased, as compared to the version used in most of the units for which there was extensive operating history.

6

EXAMPLES AND CASE HISTORIES

This section provides examples intended to illustrate how the guidance provided in both EPRI TR-106439 and this supplementary document can be applied for items of varying complexity and safety significance. The examples begin with a flow indicating controller and conclude with a Main Steam and Feedwater Isolation System (MSFIS) upgrade, illustrating how the level of effort required for the dedication activities increases as the complexity and safety significance of the item increase. These examples also attempt to incorporate some of the everyday realities encountered in nuclear plant upgrades. Background material is provided in the examples to help in understanding the bases for critical characteristics selection and verification.

6.1 LPSI Flow Indicating Controller

6.1.1 Overview

This example illustrates a case similar to that of example 6.1 in EPRI TR-106439 in that the upgrade involves a fairly simple application in which the safety significance is relatively low. In this case, the plant operating experience with the commercial device, coupled with a previous survey and widespread successful operating history, provide adequate assurance without the need for an application specific commercial grade survey or an application specific detailed review of the device's internal design and development process. A prior survey and critical digital review of the controller for another plant application are considered to encompass this application. A similar approach might be used if another utility has performed a survey and detailed review of the device to be dedicated and shares the results.

The utility is performing an upgrade in which an obsolete analog low pressure safety injection (LPSI) system flow indicating controller is to be replaced with a microprocessor-based flow indicating controller. The Reg. Guide 1.97 related function of the device is to indicate to control room operators the value of a single variable, LPSI pump flow. A second, non safety-related function of the controller is to control LPSI pump flow for shutdown cooling. To satisfy the independence requirements of IEEE 7-4.3.2, the controller software is treated as safety-related. There is to be one indicating controller installed in each of the LPSI system's redundant loops. The instrument loops are qualified, independent, and separated.

6.1.2 System

There are two low pressure safety injection pumps. During normal plant operation the LPSI system is maintained in a standby mode with all of its components lined up for emergency injection. During this time none of the system components are operating. Following an accident which results in a safety injection actuation signal, the LPSI pumps automatically start, and low pressure injection valves automatically open. Flow from each of the LPSI pumps is monitored by the operators using the flow indicating controller that is being upgraded. The LPSI flow indication is a Type D, Category 2, Reg. Guide 1.97 parameter. Reactor level, LPSI pump motor currents, loss of LPSI pump power alarm, and refueling water storage tank (RWST) level provide diverse information from which to infer LPSI pump operation.

The LPSI pumps serve two functions. The first is injecting borated water into the primary coolant system during an emergency involving a large pipe rupture. The second function of the LPSI pumps is to provide shutdown cooling flow through the reactor core and shutdown cooling heat exchangers. These functions do not require a fast response flow-indicator. There is local control for the pumps and valves, and the control function for these components is not time critical.

6.1.3 Flow Indicating Controller

The existing flow indicating controller is an analog fixed scale, moving needle display, with operator selectable automatic-local and manual modes of operation. The controller receives a process variable (PV) input, which is the shutdown cooling flow. The controller compares this input to an operator selected setpoint and produces an output signal which is based on the deviation between the actual shutdown cooling flow and the desired flow.

The modes and signals described above are displayed on the controller. The scale plate is marked from 0 to 8000 gpm. The process variable is displayed by a moving needle on the left side of the scale which moves toward the top of the scale on increasing flow. The Set Point (SP) is displayed by a moving needle on the right side of the scale. Below the level scale is a horizontal indicator which displays the output signal as 0 to 100%, increasing left to right. The controller has a light in the upper right hand corner which is lit when it is in automatic.

The existing controller has a thumbwheel for manual setting of the SP value, a knob for manually setting output, and a slide bar located below the output indicator which is used for shifting between modes. To shift modes, the controller is partially withdrawn from its case to expose the switches needed to allow comparing and matching signals. The controller is a basic proportional/integral/derivative (PID) single loop controller. In this application the derivative function is not used.

A commercial off-the-shelf controller with an indicating capability, from an established manufacturer, is chosen as the replacement device. It provides the needed capability, is readily available, is widely used, and is used for other applications in the plant. Comparison of the application requirements to the vendor's specifications indicates that the requirements are within the vendor-specified performance limits. Thousands of these controllers have been in service for several years in a number of industries, and vendor failure report tracking indicate they have been reliable. Also, this controller has been used in several other plant applications. It received an in-depth critical digital review for one of these applications. The review scope encompassed the controller capability needed for this application.

The replacement controller is also to be a single loop PID controller with an indication capability. For this application, the controller will be configured to use a factory loaded single loop, basic PID control program. By using a plug-in handheld configurer, the default settings are to be changed to set the scale, PV, SP, and output parameters, and the PID control settings. The existing scale range and shutdown cooling flow SP are being maintained with the new controller.

6.1.4 Controller Operation

All operator actions are performed from the front of the controller by using pushbuttons, without withdrawing the controller from its case. The pushbuttons are on the face of the controller. The buttons are used to shift between automatic and manual, and to manually change the setpoint and output. These buttons are also used to configure the controller. To eliminate the possibility of accidentally changing the control configuration by using the pushbuttons, the controller will be password protected. This password does not affect the ability to change the configuration with the hand-held configurer (plug-in).

6.1.5 Display

The replacement controller uses a gas discharge dot matrix display. The standard color is black background with orange dots. The controller uses a program called a "display handler," which is separate from the control program, to allow configuring which displays can be called up by using the two pushbuttons. The controller comes from the factory with approximately 30 different display screens loaded into ROM, which covers the range of single, two, three and four loop control programs. Each control program can be used with up to 8 displays configured into the display handler. For this application, the information available on many of these screens is not needed, and in fact could present confusing information. Accordingly, the display handler is configured with only the standard display.

6.1.6 Microprocessor

The process controller is a member of a major vendor's family of controllers. It has a main-board layout with few components, achieved through the use of an ASIC (Application Specific Integrated Circuit) containing the same basic microprocessor used in a prior version of the controller. The plant has had good experience with the prior controller.

The basic controller with no option boards is a small evolutionary step from the prior controller, with more memory, an improved display, improvements in EMI/RFI protection, and improved behavior on watchdog timeout. Also, the basic controller executes software sections which are small modifications to sections used in the prior version of the controller.

The use of any option board results in a more complex hardware architecture and activates new "memory mapping" sections of code that were not part of the prior version controller. Further, the use of an *intelligent* option board introduces another microprocessor which shares memory with the main-board processor. This is achieved with direct memory access circuitry controlled by new sections of code in the real-time kernel. However, none of these additional option boards is used in this application.

The controller memory configuration is maintained by a lithium battery that is permanently installed (i.e., soldered) into the circuit board. It can only be replaced by de-soldering its connections. It is rated for a ten year life based on a continuous small amount of current draw. The battery has been entered into a preventative maintenance replacement program to track its life.

The controller microprocessor is equipped with a watchdog timer which functions to monitor normal operation of program execution and detect when a system fault has occurred. Basically, if the control program takes more than a fixed amount of milliseconds to execute, a fault in the system is indicated, and the controller front panel display will begin to flash, indicating to the operator that a fault has occurred.

6.1.7 Software Operation Overview

On power-up the system initializes data points stored in lithium battery backed RAM in according to the user selected configuration. The RAM database establishes configuration items such as PID tuning constants, digital filter time constants, alarm setpoints, engineering units span, and display update rate. The RAM also provides "softwiring" data points which determine the control strategy, that will be used.

After initialization a wait loop begins. This wait loop is interrupted every 50 ms, starting a string of code. All executable lines of code are held as embedded firmware in a 65 Kbyte Erasable Programmable Read Only Memory (EPROM). The process variable

is sampled every 50 ms. The 4-20 mA current from the differential pressure transmitter is dropped across a 250 Ω input resistor providing a 1-5 volt signal. The signal then passes through a single-pole, analog low-pass filter.

A comparator and analog-to-digital converter perform A/D conversion through a 12 bit successive approximation technique. This results in a quantization of ½ Least Significant Bit (LSB) and an overall measurement accuracy of within ≮ 0.1% of span. This 12 bit word is then smoothed through a first order digital filter, scaled and placed in RAM.

A control algorithm is then run every Program Scan Cycle of 0.05s to 1.5s as configured by the user. In this application with Flexible Control Strategy (FIX1) enabled, single Loop PID is selected from coded function blocks. These function blocks are stored in the EPROM and "softwired" via data points stored in RAM.

When the control algorithm operation has been completed and the analog output is updated, the display program is allowed to run. The display program is also stored in the EPROM. The display program chosen is determined by the value stored in RAM. This program obtains the process variable value from RAM and generates a pattern of bits in a 1K RAM display buffer. The display buffer, display driver, and microprocessor are all contained on a single Application Specific Integrated Circuit (ASIC) chip. The display update cycle is completed once every 1 to 15 Program Scans as configured by the user.

The display driver takes the pattern of bits stored in the 1K RAM and illuminates a 96 x 48 dot matrix display. The dynamics of the display require that each element be on for only a fraction of a second. Therefore, to give the appearance of being lit steadily, the driver turns the individual elements on and off eighty times a second.

6.1.8 Performance Features

The existing controller has a measurement accuracy of $\pm$ 0.4% of span, and an indication accuracy of $\pm$ 0.8% for the process variable and $\pm$ 2% for the output. The replacement controller has a measurement accuracy of $\pm$ 0.1% of span and an output accuracy of $\pm$ 0.2% of span. An accuracy value is not given for the indication, but it is reasonable to assume that it is 0.2% of span (same as output accuracy) because it is a digital device. Accordingly, the stated accuracy values are better for the new controller than for the old.

An annunciator is provided which alarms when either LPSI pump trips. The alarm provides the operator with an indication when a LPSI pump breaker opens. This provides the operator which additional backup information related to LPSI pump flow and can be used to crosscheck the flow indicators.

6.1.9 Design Process

The utility follows the design process and licensing guidance provided in EPRI TR-102348, and uses the guidance in EPRI TR-106439 and station procedures for planning and performing the commercial dedication. Design requirements for the indicating controller are identified based on the intended application. A human factors evaluation is performed to confirm that the new controller will provide an interface that is adequate and comparable to the old controller. The utility also performs a failure analysis that provides information on important failure modes for the application. Based on this information, critical characteristics for the indicator are identified as shown in Tables 6-1, 2, and 3. Since the control function is a non safety-related function, the critical characteristics focus on the Reg. Guide 1.97 indication function.

6.1.10 Dedication Considerations

The commercial grade process control station which is used in other plant applications is selected as the indicator replacement because the plant has experience with it and is set up to maintain it. It provides the needed indication and control capabilities. The controller has a main-board layout with few components achieved with the use of an ASIC (Applications Specific Integrated Circuit) containing the same basic microprocessor used in the prior version of the controller.

The basic controller with no option boards is a small evolutionary step from the prior version, with more memory, and improved display, improvements in EMI/RFI protection, and improved behavior of watchdog timeout. Also the basic controller executes software which has few modifications to that used in the prior version.

The controller was designed from the standpoint it could be configured in a combination of ways using either the standard flexible control strategies supplied from the vendor, or using pre-defined building blocks, known as control interconnection blocks, or by using a translator language. The standard device was utilized to configure the controller as a standard indicator with a PID single loop control capability.

The vendor has ISO-9000 certification, but the controller evolved within a hardware development culture where software was treated the same way as a detailed drawing with respect to development, documentation, and responsibility for quality. Under this pre-ISO 9000 system, the object (drawing/software) was prepared by responsible people and released to manufacturing through a formal release process, at which time basic quality assurance review procedures are followed. After release, change control procedures were followed by engineering and manufacturing. Specific pre-release work methods and practices were typically set by the leaders responsible to management for delivering the object on-time with acceptable quality. Pre-release software development practices for the controller family were informal.

A prior audit of the vendor for another plant use of the controller raised a number of concerns. Software quality assurance procedures with the controller were minimal. Specifically,

- There were no software requirements or design documents.
- No documented software verification steps were performed during development and implementation.
- No documented coding standards or guidelines were applied.
- No formalized software test plan was developed and verified.

The only software documentation generated during the development process, other than the code itself, consisted of "bi-weekly" reports designed to keep management aware of progress with the project.

After the initial release and until the time of the audit, a software quality team functioned to review and report on the status of software modification requests submitted by applications engineers. Despite these prior weaknesses, the controller had built an acceptable operating history and the plant was familiar with it.

The utility decides to procure three indicators and performs the inspections, tests, and reviews described in Tables 6-1, 2, and 3. For this device and application, verification of many of the physical and performance critical characteristics is straightforward; they are successfully measured or tested on receipt. In the dependability category, verification of the critical characteristics is more subjective and, in this case, the acceptance criteria reflect the fact that the device application is simple, is software configurable only under administrative procedures after it is installed, and the safety-related application uses only two basic functions, which can be thoroughly tested.

Because of the application of the device, its successful and relevant operating history, the prior vendor audit, and the prior critical digital review, it is concluded that a detailed application specific survey and associated visit to the vendor's facility are not required. Testing and software V & V are the primary means of verification in this case, supplemented by the device's operating history. Because the device has only two functions, all the operating history is considered relevant to the planned application. The design is stable and this device represents the third generation in a family of similar controllers, all of which are digital. Also, the wiring design changes to resolve an EMI problem with another plant application of the controller are incorporated in this application.

A relatively thorough software V & V review is performed because of the prior audit findings. This includes a review of the prior vendor audit and reviews of the software

for the prior application. For this application the following additional V & V reviews are performed:

- Application requirements analysis
- Interface requirements analysis
- Requirements traceability analysis
- Architecture review
- Configuration review
- Stress tests
- Documentation evaluation
- Installation configuration

The following hazards and failure modes are evaluated:

- Electromagnetic Interference (EMI)
- Inadvertent Configuration Changes
- Undetected CPU Failure
- Power Loss
- Power Restoration
- Potential Software Defects
- Loss of Input Signal

The failure analysis finds that, because of the application, the device has only a few different external failure modes that encompass all the failure modes of the internal components. The device does not automatically actuate any safety related plant equipment. Behavior of the indicator under anticipated abnormal conditions (e.g., loss of input signal) can be verified by testing. Confidence that there is a sufficiently low probability of any other unexpected failures of significance (e.g., silent failures that could give incorrect readings) is based on the utility testing of the device, the relevant operating history, and the normal periodic checks and calibrations that are performed on the instrument. In addition, the indicated variable can also be inferred using other instrumentation available to the operators.

Based on these results, the extensive operating history, the plant experience in other applications, and the consideration that there is local control for the pumps and valves, and the control function is not time critical, the controllers are installed and a commercial dedication package is completed documenting the critical characteristics, acceptance methods, and activities used to dedicate the device, including the basis for engineering judgments made. In this case, the application of the indicator, coupled with its demonstrated stability and reliability in more complex applications, prove key to establishing reasonable assurance that the device will perform its safety function.

Table 6-1.
LPSI Flow Indicator — Physical Critical Characteristics

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

Table 6-2.
LPSI Flow Indicator — Performance Critical Characteristics

Performance Critical Characteristic	Acceptance Criterion	Method of Verification
Functionality • Accuracy • Range • Response time	 Per utility specification 0-8000 gpm (4-20 ma) operating range Per utility specification	Utility's receipt inspection tests (performed for all procured indicators, not just a sample) (Method 1)
Environmental Compatibility • EMI • Temperature	 Per utility specification (e.g., using EPRI TR-102323) Per utility specification based on control panel location (mild environment)	A third-party test lab report for one of the controllers is in the plant records from a prior application. All procured controllers are inspected to ensure that the tested controller is equivalent to those reviewed for the characteristics being verified (Methods 1 & 2).
Behavior under abnormal/faulted conditions • Loss of signal • Loss of power • Signal over/under range	Detectable by operator when reading the indicator	Receipt inspection tests (Method 1)

Table 6-3.
LPSI Flow Indicator — Dependability Critical Characteristics

Dependability Critical Characteristic	Acceptance Criterion	Method of Verification
Built-in quality		
• Quality of design & manufacture	Inspection and test results meet their acceptance criteria Visual inspection shows use of good commercial manufacturing practices Successful and relevant product operating history These taken together demonstrate adequate quality of the device	Inspection and testing by utility (Method 1) Based upon success of operating experience with the model being used in this and other plant applications. (Method 4).
• Failure modes and failure management • No failure not readily detectable by operators prior to taking readings on the controller.	Failure modes are adequately addressed based on failure analysis and testing. (Note: Failure analysis is also used to help determine whether unreviewed safety questions exist per 10 CFR 50.59 -- see EPRI TR-102348 and NRC Generic Letter 95-02.)	Failure analysis identifying failure modes and assessing their significance
• No adverse interaction between the non-safety control function and the Reg. Guide 1.97 indication function that could compromise the indicator's operability due to failure in the control software		Vendor survey and review of product operating history to help verify absence of specific critical failures. Challenge testing designed to test for possible critical failure modes in normal operation (operation over entire range including slow and fast sweeps plus steady-state readings) and under abnormal conditions (e.g., degraded power supply voltage, out-of-range input, noisy signal, etc.). Critical digital review of the processor and software for another application are also credited.
Problem reporting	Vendor has error-reporting procedures and will provide reporting to utility.	Agreement with vendor on error-reporting procedures.
Reliability	Successful operating history	Review of product operating history for demonstrated reliability.

6.2 Recorder with internal microprocessor

6.2.1 Background

This example illustrates a case in which an analog device is being replaced with a newer "smart version" of the device offered by the vendor. The microprocessor based "smart version" has limited operating history. Accordingly, to obtain adequate assurance, a commercial grade survey and detailed review of the device's internal design and development process are necessary.

For this example a recorder is selected. However, a similar approach would likely be applicable to other "smart" device upgrades for indicators, transmitters, relays or other similar devices.

This example also is intended to illustrate the "digital delta" required to dedicate a "smart" device versus the dedication of the analog version as can be found in many EPRI Commercial Grade Item Joint Utility Task Group (JUTG) Technical Evaluations. In particular, the analog recorder critical characteristics of JUTG Technical Evaluation CGICR01 are noted in the critical characteristics tables to illustrate the "digital delta" in critical characteristics. The additional activities required in the dedication of a "smart" device are also discussed in Section 6.2.5 on Dedication Process. Basically, the additional complexity, functionality and failure modes of the "smart" device versus the analog device must be addressed.

6.2.2 Device Overview

The utility is performing an upgrade in which an existing analog recorder, used as a safety system recorder, is to be replaced with a microprocessor-based device. The function of the device is to record the value of a single variable. Two of these recorders are used to provide redundant readout for the variable. The redundant instrument loops are qualified, independent, and separated. A commercial, off-the-shelf digital "smart" recorder from an established manufacturer is chosen as the candidate replacement device because it provides the needed functionality, is readily available, and is becoming widely used. It is a single-function device but has software configurable features. A fixed 4-20 mA input is used. Comparison of the application requirements to the vendor's specifications indicates that the requirements are within the vendor-specified performance limits. Only a few hundred of these indicators have been in service for the last few years in a number of industries (pharmaceutical, chemical process, etc.) but they have developed a reputation for reliability.

6.2.3 Recorder Operation

The basic operation of the "smart" recorder is similar to that of the analog recorder. Its function is to automatically plot or draw on stripchart paper, in a form of a continuous curve, the values of one or more measured variables, generally against time. The variable being measured is drawn on rectangular coordinates, generally with time in one axis and measured variable (s) in the other axis. The addition of the microprocessor allows additional functionality such as more capability for input parameter processing, ranging and scaling, variable selection, digital value printouts, annotating and self diagnostics.

6.2.4 Dedication Process

The utility follows the design process and licensing guidance provided in EPRI TR-102348, and uses the guidance in EPRI TR-106439 and station procedures for planning and performing the commercial dedication. Design requirements for the recorder are identified based on the intended application. The utility also performs a failure analysis that provides information on important failure modes for the application. Based on this information, critical characteristics for the recorder are identified as shown in Tables 6-4, 5, and 6.

The utility procures three recorders and performs the inspections, tests, and review described in Tables 6-4, 5, and 6. For this device and application, verification of many of the physical and performance critical characteristics is straightforward; they are successfully measured or tested on receipt. In the dependability category, verification of the critical characteristics is more subjective and requires more effort. Since the recorder has not yet established an adequate operating history, a survey at the vendor's plant, including a detailed review of the software development process and configuration control is performed. The review also involves some code inspections to examine code architecture and design practices. The review indicates that the recorder vendor follows industry guidance for computer system development and maintains a well documented design file, including thorough software documentation.

A failure analysis for the recorder finds that the recorder has a limited number of different external failure modes that encompass all the failure modes of the internal components. Also, the device does not automatically actuate any plant equipment. Behavior of the indication under anticipated abnormal conditions (e.g., loss of input signal) can be verified by testing. Confidence that there is a sufficiently low probability of any other unexpected failures of significance (e.g., silent failures that could give incorrect readings) is based on the utility testing of the device, the vendor survey and detailed review of the recorder's design and development process, and the normal periodic checks and calibrations that are performed on the device. Also, the recorded variable can be obtained from the plant process computer.

Based on these results, the recorders are installed and a commercial dedication package is completed documenting the critical characteristics, acceptance methods, and activities used to dedicate the device, including the basis for engineering judgments made. In this case, because of the limited operating history of the recorder, a thorough review of the recorder is relied upon to establish adequate assurance that the device will perform its safety function.

Table 6-4.
Smart Recorder — Physical Critical Characteristics

Physical Critical Characteristic	Acceptance Criterion	Method of Verification
Configuration • Manufacturer/ Model/Nameplate Data* • Software revision number • Dimensions* • Mounting* • Weight*	 Per mfr. published data Vendor software revision # Per mfr. published data Per mfr. published data Per mfr. published data	Receipt inspection verifies these characteristics. Also, the vendor survey provides detailed information on the vendor's configuration control practices and software version tracking. The utility records the software (firmware) revision number for the units that are received and tested, so as to trigger a re-evaluation if different revision levels or part numbers are received in future procurements.
Interfaces • Input signal* • Power*	 Per mfr. published data Per mfr. published data and per utility specification	Receipt inspection tests
HMI • Writing area* • Writing paper* • Number of Pens* • Ink Colors* • Operating position*	 Per mfr. published data Per mfr. published data Per mfr. published data Per mfr. published data Per mfr. published data	Receipt inspection tests

* Denotes critical characteristics listed in the JUTG CGI Technical Evaluation for analog recorders

Table 6-5.
Smart Recorder — Performance Critical Characteristics

Performance Critical Characteristic	Acceptance Criterion	Method of Verification
Functionality		
• Writing System*	Per mfr. published data	Utility's receipt inspection tests (performed for all procured recorders, not just a sample)
• Accuracy*	Per mfr. published data	
• Voltage/Current Range*	Per mfr. published data	
• Linearity*	Per mfr. published data	
• Power Requirements*	Per mfr. published data	
• Response time	Per utility specification	
Environmental Compatibility		A third-party test lab report for one of a small sample of the recorders in a lot that are tested; the utility inspects all procured recorders to verify homogeneity of the lot and to ensure that the tested items are equivalent to those not tested, for the characteristics being verified.
• EMI	Per utility specification (e.g., using EPRI TR-102323)	
• Seismic	Per location response spectra	
• Temperature	Per utility specification based on control panel location (mild environment)	
Behavior under abnormal/faulted conditions	Detectable by operator when reading the recorder	Receipt inspection tests
• Loss of signal		
• Loss of power		
• Signal over/under range		

Table 6-6.
Smart Recorder — Dependability Critical Characteristics

Dependability Critical Characteristics	Acceptance Criterion	Method of Verification
Built-in quality		
• Quality of design & manufacture	Inspection and test results meet their acceptance criteria Visual inspection shows use of good commercial manufacturing practices	Vendor survey, detailed design review and inspection and testing by utility
• Failure modes and failure management	Failure modes are adequately addressed based on failure analysis and testing. (Note: Failure analysis is also used to help determine whether unreviewed safety questions exist per 10 CFR 50.59 -- see EPRI TR-102348 and NRC Generic Letter 95-02.)	Failure analysis identifying failure modes and assessing their significance. Challenge testing designed to test for possible critical failure modes in normal operation (operation over entire range including slow and fast sweeps plus steady-state readings) and under abnormal conditions (e.g., degraded power supply voltage, out-of-range input, noisy signal, etc.)
Problem reporting	Vendor has error-reporting procedures and will provide reporting to utility.	Agreement with vendor on error-reporting procedures.
Reliability	Low failure rate observed in testing.	Challenge testing, vendor testing and results of vendor survey to assess built-in quality.

6.3 Auxiliary Feedwater Controller

6.3.1 Background

This example illustrates a case in which an aging analog control system is to be replaced with a digital control system. An attempt is made to use commercial grade equipment. However, inadequate examination of the equipment and vendor early in the upgrade result in a failed attempt to successfully dedicate the new digital control system. Time and money are wasted. The utility must start over on the upgrade and delay its installation for a refueling cycle.

6.3.2 Design and Dedication Process

A utility is faced with increasing corrective maintenance on an auxiliary feedwater (AFW) control system. The analog control system is a series of modules that provide signal conditioning and PI control on S/G level. The vendor of the existing analog control system has announced retirement of the product line, and parts and service support will end the following year. The system has experienced some instabilities and transients during surveillance testing that have been difficult to fix. The system is safety related.

A salesman from a commercial control system vendor has visited the utility and offered to provide a replacement "plug and play" digital control system at a reasonable price. The utility likes it, and is successful in writing a sole-source justification and convincing management to buy one copy of the system for evaluation (one is needed for each unit, plus a third for the simulator). The sample system is put together by the vendor and delivered to the plant, where it is set up in a lab and a detailed application database is developed largely through trial and error. After running some static and dynamic tests, it appears that the system will perform reliably. A purchase order is initiated to buy three more copies of the system. At the same time, a plant mod package is initiated.

A procurement engineer is assigned to the purchase order and a Lead Design Engineer (LDE) is assigned to the plant mod package. They have never heard of the project before, and didn't know there had been an evaluation copy of the system in the lab. They sit down and begin to compile requirements. They see that the vendor is not Appendix B, so they begin work on a commercial grade dedication strategy. From their plant design documents, they assemble functional and performance requirements. From their digital upgrade standards, they apply EMI/RFI and software quality assurance (SQA) requirements. They write a detailed specification for the project and send it to the vendor.

The vendor balks at the specification. Nobody ever told him about nuclear safety related equipment standards being imposed. He just sold a COTS system to a plant engineer, and as far as he is concerned, he is under a verbal obligation to sell three more just like the evaluation system. The system comes ISO-9000 certified, and nothing more. After consulting with his management, he is ready to "no-bid" the project and let the utility try their luck somewhere else. The plant engineer still likes the system, and is convinced it is the right product at the right price. The plant engineer insists that design and procurement find a way to make it work.

It takes some haggling, but the LDE and procurement engineer convince the vendor he is under no obligation to meet federal laws for safety related applications in nuclear power plants. The utility bears all responsibility for the safety of the system, including QA and reportability requirements. An audit should confirm that the vendor has a bullet-proof commercial QA on the system; the utility only has to verify everything, and

send the system to a third party "shake and bake" lab for additional hardware testing. After all, the vendor has ISO-9000, which should get the system 90% of the way to meeting all requirements. The utility will handle the rest. And, the utility will gladly pay the vendor for his time and trouble during the audit. The vendor reluctantly agrees to the audit.

The utility assembles a commercial grade survey team, with an ANSI certified lead auditor, the LDE, the procurement engineer, and a software specialist. They go to the vendor's facility for a three day survey, with a detailed list of critical characteristics to verify. It turns out a NUPIC team had been in previously. The NUPIC team looked at the more generic QA requirements such as document control, procurement control, and material control. They did not look at software quality assurance (SQA), so the utility team decides to spend most of their time in that area.

The first day goes well. The team meets with senior management from engineering, QA, manufacturing and marketing. The vendor's management team opens all doors and lines up interviews with the engineering staff. Procedures are made available, and a tour of the facility is provided. The culture of the company looks impressive, and the procedures give the impression that the vendor is fully committed to a solid software development process.

The second day doesn't go so well. The product line that is being surveyed was developed about the same time the company went ISO-9000. The software is 95% legacy code from previous product lines, and some of that code is dead because of the relatively new architecture of the new system. There is little evidence of any formal methods or documentation on the software. Requirements documents are vague, and establishing traceability from a given requirement to a validation test is very difficult. The engineering manager says his engineers are committed professionals with a high level of integrity, and there isn't anything in the code that wasn't tested at white- and black-box levels. Interviews with the design engineers confirm that exhaustive analysis and testing were done, but there is very little documentation to objectively confirm it.

The survey team shifts the focus to configuration management. A firmware "build" is witnessed by the team. A software technician pulls a diskette from a filing cabinet, demonstrating security and labeling of the various versions of the code. He puts it in a PC, and runs some utilities. The team reads the code (banner sections only, to verify version). They compile and link the source, and ultimately burn a PROM copy of the run-time version. They carry the chip down to a lab area and install it on the motherboard of the system. They start the system and observe it running. The software specialist observes some differences on the MMI between what he sees in the vendor's lab and what he saw on the evaluation copy of the system back at his own lab. The vendor says that should be expected, since he is constantly upgrading the firmware. New requirements come up all the time, not to mention problem fixes. Configuration control between engineering and production appears loose.

The survey team moves on to the vendor's error discovery, tracking and corrective action program. They find a database in the customer service department that is used to track customer calls and product returns. A unique number is assigned to each call, and service technicians keep an accurate database. All problems are tracked until they are resolved, then they are closed and kept as QA records. The survey team asks if any software related problems have been discovered by any customers. The service techs say they don't really know, that they refer problems they can't fix to the engineering department. There have been a few calls referred to engineering.

Over in the engineering department, there is another database for tracking product modifications. All software and hardware mods are controlled via this database. The survey team tries to link the customer service database with the engineering database, to verify that a field problem that was sent to engineering was properly handed off, tracked, and resolved via an appropriate change. The data is confusing, difficult to link, and has some apparent errors. One field problem in particular is unresolved. In this one case, where the system behaves erratically under certain conditions, customer service sent the problem to engineering, who told customer service to send another copy of the product to the customer. It turns out the problem is not really fixed yet, although customer service has closed out the issue in their database. Engineering is having trouble repeating the problem, and it is sitting on a back burner. They are pre-occupied with launching a new product line.

The engineering database is researched further, and it turns out more than one customer service call is linked to the same problem, and that there are several unresolved problems with the software. Engineering works on problem fixes when they get a chance. Some of the problems are categorized as bugs, when they are really major problems under certain conditions. Some of the problems are several years old, and they have been put on hold pending release of the new product line, which will fix everything. The marketing department has been told by engineering to concentrate on selling the new product line when customers call with complaints on the old product line.

Finally, the survey team attempts to cross-reference software releases from engineering with the software under configuration control. They find that the latest approved release from engineering doesn't match the software build they observed earlier in the survey. Version 2.2 is being installed on new systems coming out of the factory, and engineering thinks version 2.3 is in production. Version 2.3 fixes several bugs and one major defect over version 2.2.

The survey team closes on day three with an exit meeting. They discuss preliminary findings with management, and commit to providing a written report within two weeks. The vendor's management team commits to improving their processes.

Back at the plant, the survey team discusses the findings with the plant engineer and plant management. To date, over a year of product evaluation has gone into the project. Close to $100K has been spent on engineering labor, the evaluation system, and the survey. Project deadlines are coming up fast. The AFW system really needs an upgrade soon, and four months are left before the next outage when the upgrade is to be installed. The LDE asks for a two week period to finalize the product evaluation and make a decision on whether or not to proceed with the chosen system.

The LDE begins some detailed testing in the lab. An application has already been set up in the lab that meets the AFW control application functional and performance requirements, so the LDE works on identifying failure modes and effects. He puts the system in various modes, and forces failures on inputs. Several times the system crashes, and he is forced to reboot. He finds that the system outputs (AFW control valve and AFW pump speed) behave erratically under various failure modes, which is unacceptable. He also finds that modifying the application database to do things like validate inputs and clamp outputs on certain failure modes doesn't fix all of the problems. There are some problems like stack overflows, memory allocation errors and watchdog time-outs that are more a function of the real-time kernel, or operating system. It becomes apparent that to make a robust application, it will be necessary to spend a good amount of time with the vendor's engineering staff. Custom changes to the operating system appear to be necessary.

The LDE meets with the project team. They discuss all of the issues on the system, and decide to recommend rescheduling the project for the next outage and start over with a new vendor. This time, the system specification will be let to numerous vendors for commercial bid. The vendors selected to receive the specification include Appendix B vendors, COTs vendors, and third-party integrators. As much emphasis will be placed on the product as the application. SQA and operating system characteristics will be thoroughly evaluated, via a Critical Digital Review (CDR), and the application development will come later in the project using the utility's Appendix B design controls.

Utility management reluctantly agrees with the project team's recommendations. Over $100K will be lost, as well as another two years until the next refueling outage when a new system can be installed. Lessons learned from this project are applied to other projects around the plant.

6.3.3 Lessons Learned

The key lesson to be learned from this example is the need to understand what is required to use new equipment that is digital and equipment that is commercial grade. Guidance provided in this report, TR-106439, and TR-102348 can help prevent situations such as the one documented in this example.

6.4 Multiple Computer System

6.4.1 Background

This example illustrates another step up in complexity and safety significance as compared to the simpler devices discussed in Examples 6.1, 6.2, and 6.3. The example illustrates a case in which a system utilizing multiple computers is used to perform a set of functions. It involves the replacement of an Inadequate Core Cooling Monitoring System (ICCMS). The ICCMS to be replaced is a digital system which is becoming obsolete. The dedication acceptance is based on extensive testing, analyses, evaluations, audits, design and implementation oversight and thorough documentation.

6.4.2 System Overview

Regulatory requirements for the Inadequate Core Cooling Monitoring System (ICCMS) are provided in Regulatory Guide (RG) 1.97 and Section II.F.2 of NUREG-0737. The purpose of the ICCMS is to provide the reactor operator with a continuous indication of the thermal-hydraulic state within the reactor during an event leading to and away from Inadequate Core Cooling (ICC).

The typical ICCMS sensor package consists of the following measurements:

1. Hot and cold leg temperatures

2. Pressurizer pressure

3. Core Exit Thermocouples (CETs)

4. Reactor Vessel Level Monitoring System (RVLMS) probes.

The sensors are normally integrated into a system designed to monitor, display, trend and log parameters associated with the approach to and recovery from ICC. A functional diagram of the typical ICCMS is shown in Figure 6-1.

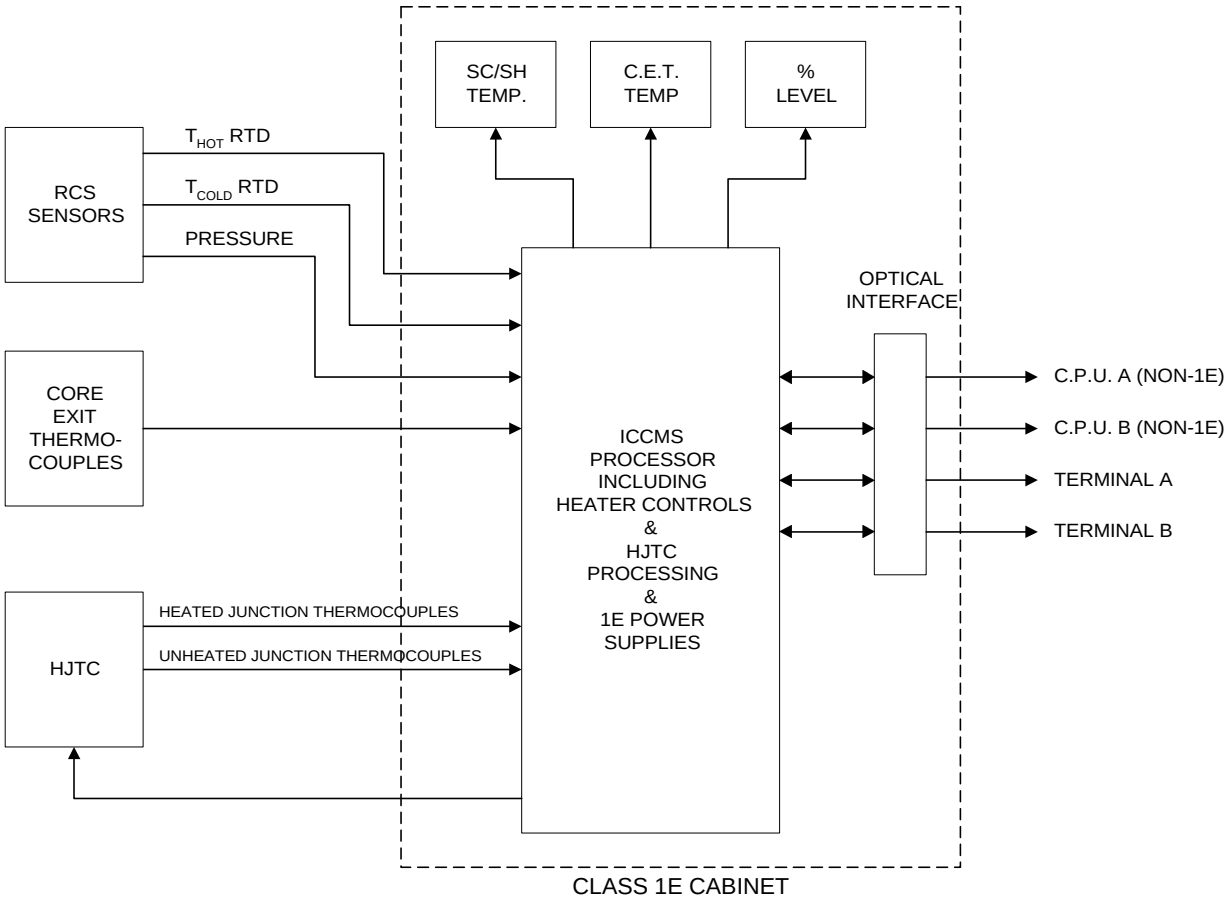


Figure 6-1.
ICCMS Functional Block Diagram — Train A (Train B — Similar)

The replacement ICCMS of this example replaces the existing ICCMS cabinets internal hardware and software with new hardware and software. The replacement ICCMS was designed to perform all ICC monitoring functions, including Reactor Vessel Level, Saturation Margin, and Core Exit Temperature, as before. Communication with the plant process computer is to be changed to 'broadcast' only, so no 'handshaking' between the R. G. 1.97 Category 1 ICCMS and the non-QA plant computer will occur. An alarm window is also to be added to the control boards to annunciate on ICCMS Trouble. All process inputs are to remain unchanged as a result of the modification. The change is required to address parts obsolescence and equipment reliability concerns, and to re-establish design basis and software configuration controls.

Functionally, the replacement ICCMS is to provide the same indication and alarm of ICC parameters as before. A single microprocessor will perform all processing functions in each channel. The replacement system incorporates enhancements made available by the use of newer microprocessor and display technology. The replacement system meets or exceeds the design and qualification requirements of the existing

ICCMS, including environmental and seismic. In addition, an evaluation of EMI/RFI susceptibility was performed which compares results of testing performed on the replacement equipment with the environment mapped for the existing cabinet location. The main microprocessor had been qualified for use previously for another application which encompassed the requirements of this application. Verification and Validation (V&V) of the hardware and software design implementation was completed by the supplier.

The replacement microprocessor system is to perform all data acquisition, processing, and display functions currently performed by the existing two microprocessor system. The existing two microprocessor system used a separate computer to process and provide level measurement. There is to be no change to existing process input and output signals and field wiring except for the addition of an ICCMS Trouble Alarm annunciator output for display on the main control board, and restoration of the process input signal cable shield drain wiring.

The RVLMS functions are also performed by the new microprocessor. Acquisition of heated and unheated thermocouple input signals, and cold reference junction compensation is to be performed as before. The heater control function is enhanced to provide individual heater control to each of eight heaters in the sensor assembly. This reliability enhancement prevents the loss of a string of four heated junction thermocouple heaters should a heater open, or a heater controller failure occur. The old system utilized two (2) controllers, one for powering each of two 'strings' of four, series connected heaters. The heater power control function algorithm remains unchanged.

The replacement microprocessor systems will process all CET inputs, and RCS pressurizer pressure and temperature analog input signals as before. Data is transmitted from the ICCMS via fiber-optic modem to the plant computer for primary display of ICC information as before, except the data is 'broadcast' on a continuous basis about every 3 seconds. The modem at the plant computer (receiving) end of the datalink is to be replaced to match the replacement ICCMS fiber-optic output modem. Data link transmission speed is increased from 9600 to 19200 bps. The previous 'handshake' implementation is eliminated to prevent possible unacceptable interaction with the QA Category 1 ICCMS should the non-QA plant computer data link experience problems.

The local digital display of ICC information is to be replaced with a local display unit consisting of a 16 color active matrix LCD flat panel touchscreen serial graphics terminal. The display is driven by the ICCMS microprocessor.

Diagnostic routines are incorporated in the new system to continuously check data integrity, and perform algorithm and calculation checks. The new system selected also incorporates continuous auto-calibration to an independent, precision voltage reference, and was evaluated by the supplier for stability over 24 month (30 months maximum)

fuel cycles. The system diagnostics will alarm prior to auto-calibration adjustments exceeding a pre-determined value. A watchdog timer also serves to indicate system faults. Diagnostics are also provided to assist in performing periodic maintenance tasks, or troubleshooting system errors should they occur.

6.4.3 Up Front Considerations

Prior to proceeding with the procurement and design activities, an assessment of available hardware and software technologies is performed. First, a platform is selected for consideration based on maturity, capability, and previous utilization. A mature platform is selected with consideration for near term obsolescence, as much as practicable. This platform had been previously utilized for a QA Category 1, commercial nuclear plant reactor protection system core protection calculator. A V&V of the platform is then performed to establish suitability for the task. The utility also considers the vendor experience, capabilities, and qualifications for completing this task.

6.4.4 Hardware Related Dedication Activities

6.4.4.1 Equipment Description

The ICCMS equipment is assembled as a simplified system. The main computer assembly (shown as μP chassis in Figure 6-2) had been previously qualified for another application and is not subjected to the testing. The computer is located outside of the environmental chamber and off the seismic table. The computer is programmed to run a simplified version of the ICCMS program. This allows for the functional verification of the system during the qualification testing. The simulation testing also qualified the system's interconnecting cabling. The heater control panel outputs were wired to a set of 8 load resistors which were used to simulate the actual loading of the heater control panel. The annunciator panel outputs were loaded with a 125 VDC voltage source, with one output loaded to over 1 amp and the other outputs loaded at lower currents. A personal computer was used to observe and capture the plant computer data link information. This equipment was located outside of the environmental chamber or off the seismic test table. Figure 6-2 illustrates the Test Set-up.

The test specimens were the following:

- The Local Display Unit (LDU) was a nineteen-inch wide rack-mounting chassis, fourteen inches high and approximately six inches deep. It has an active matrix color LCD flat panel display which communicates through an RS232 port and has a screen viewing area of approximately 10.4" diagonal.

- The Terminal Server was a nineteen-inch wide rack-mounting chassis, one and three quarters inches high and approximately twelve inches deep. This device uses an ethernet input connection and converts it to 8 serial ports for use with the plant computer data links and user diagnostic terminal data link.

- The Modem Panel was a 10″ x 8″ x 6″ assembly. It contains Fiber Optic Modems. It weighs 3 pounds.

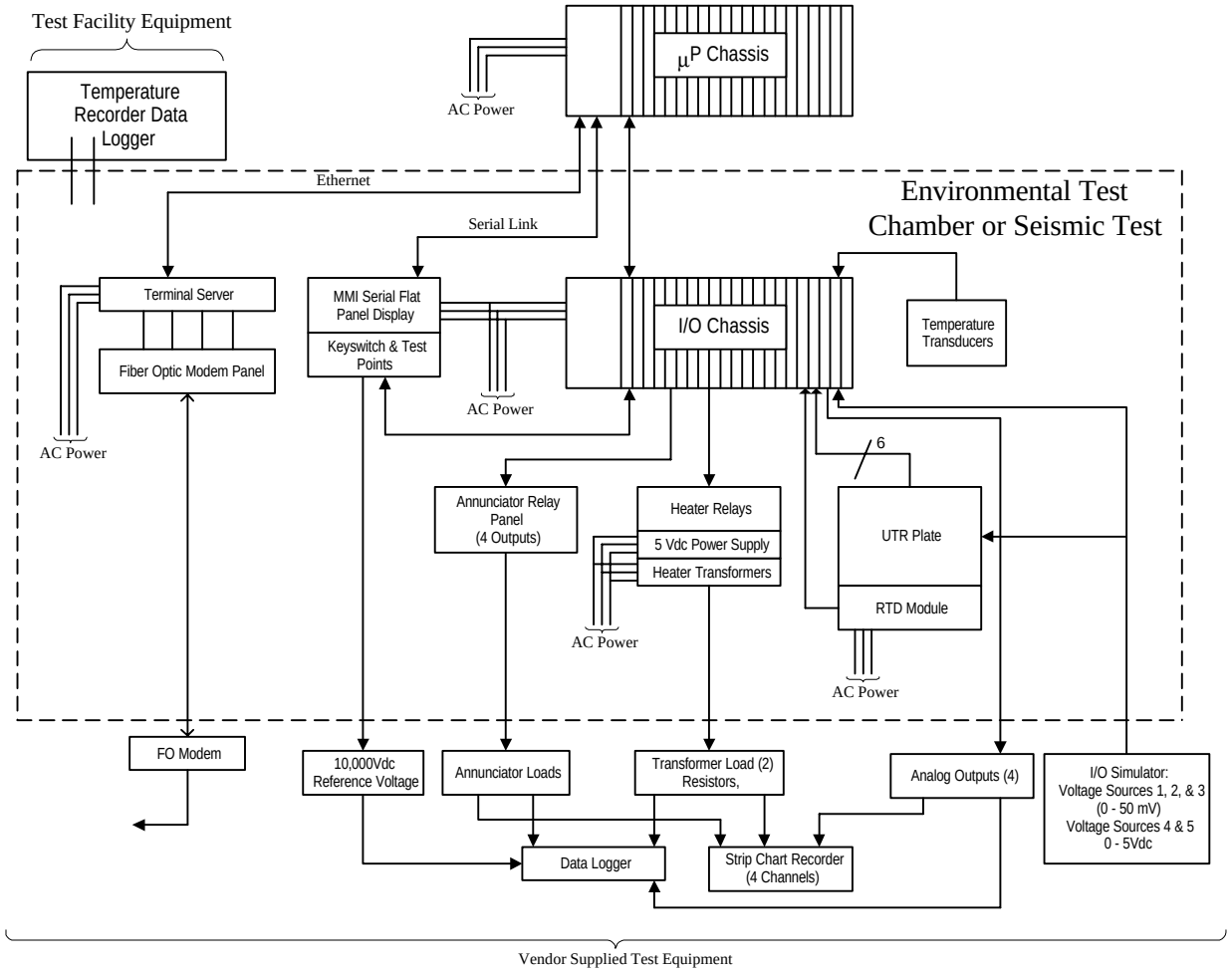


Figure 6-2.
ICCMS Test Configuration

- The computer I/O chassis was a nineteen-inch wide rack-mounting chassis, seven inches high and approximately eleven inches deep. It contains a power supply module and a full complement of circuit cards. It weighs twenty-five pounds.

- The Universal Temperature Reference (UTR) was a nineteen-inch wide rack-mounting chassis, fourteen inches high and approximately six inches deep. The assembly also contained an RTD reference assembly which is mounted to the rear of

the UTR. The UTR provides the cold reference junction compensation signals for all thermocouple inputs.

- The Heater Control Panel Assembly was a twenty-three inch wide panel, eighteen inches high and approximately five inches deep. This panel contained the step down transformers and solid state relays used to provide and control power out to the heaters for the HJTC system portion of the ICCMS. It also contains the 5 volt logic power supply for the heater logic and watch dog timer (WDT) circuits. It weighs approximately 30 pounds.

- The Test Panel Assembly was a nineteen inch wide plate, 5 inches high. It contains the Test Mode Bypass Switch, and Test Panel Connectors for input and output voltages. It weighs 3 pounds.

- The Annunciator Relay Panel Assembly was a 10″ x 8″ x 6″ enclosure which contains the 125 vdc solid state relays. It weighs 10 pounds.

- The Cabinet Temperature Sensors (2) were approximately ¼″ x ½″ x ½″, and weighed a few ounces.

6.4.4.2 Hardware Dedication Overview

Dedication of the ICCMS equipment involved a combination of testing, use of previous qualification testing, and analysis. ICCMS equipment qualification testing was conducted to satisfy the requirements of the plant site as well as seismic requirements to satisfy future installations. For the tests, the components remained connected as a system to demonstrate their ability to function during event conditions. The tests were performed by a national test laboratory. The testing laboratory was chosen to perform the testing because the tests specified required extensive test equipment and facilities as well as the services of engineers trained in environmental and seismic testing. Test procedures specified how the test specimens were to be exposed to the specified temperature, humidity and seismic environment. Strip chart recorder printouts were retained as part of the design files for future audit purposes.

6.4.4.3 Hardware Dedication Analyses

6.4.4.3.1 Environmental Analysis

The ICCMS equipment is to be located in the controlled environment of the existing ICCMS cabinet which is subject to mild environmental requirements. The environmental test profile represents the worst case internal cabinet environment for the external environment and cabinet heat load.

6.4.4.3.2 Seismic Analysis

A seismic analysis is prepared to demonstrate that the ICCMS is seismically qualified for its intended use. The enclosure in which the system was to be installed is seismically qualified previously to a generic Required Response Spectrum. An analysis compared the tested cabinet with the same enclosure containing the ICCMS to determine the differences in their characteristics and their impact on the qualification. The analysis examined the potential impact of the ICCMS installation on the stresses and mounting reactions of the previously qualified enclosure. The analysis also addressed the procedure for determining the amount of overtesting that occurs when a test specimen is subjected to more severe seismic inputs than it could be expected to experience at an actual installation. This information was applied to the test data to determine the greatest seismic responses that the equipment would experience. The results were compared with the test results for the ICCMS components. The main computer chassis was tested previously and the test results were compared to the requirements of the ICCMS cabinet. The results indicated that the responses of the postulated seismic event would not exceed the responses to which the ICCMS components were qualified. The analysis demonstrated that the ICCMS was seismically qualified for its intended use.

A seismic analysis of the Local Display Unit (LDU) to the RRS of the plant site main control board was also performed, and concluded the LDU assembly was qualified for use in the main control board as a Remote Display Unit (RDU).

6.4.4.3.3 EMI Analysis

An analysis for the Electromagnetic Interference (EMI) effects on the system was prepared. It contained information regarding the susceptibility of the system to EMI and documented the acceptability of the system.

6.4.5 Software Related Dedication Activities

6.4.5.1 Computer Code Description

The ICCMS software consists of previously developed software and user application software. The previously developed software was designed for the commercial grade main computer used in the ICCMS. The ICCMS also utilized other components from third party vendors which contain software. These included color LCD touchscreen displays and Terminal Servers. User Application software is software that was specifically designed by the supplier for the ICCMS upgrade project.

The ICCMS application software provides the processing and display of Inadequate Core cooling (ICC) instrument signals to detect the approach to, the existence of, and

the recovery from ICC conditions. The software also drives a backup display for the variables transmitted to the plant computer for the primary Safety Parameter Display System (SPDS). With the exception of non-volatile memory input/output, all user application software is coded in the C programming language for implementation on ICCMS computers. Read and write routines to non-volatile memory are coded in assembler language.

6.4.5.2 Software Design Methodology

The ICCMS application software for Channels A and B was designed in accordance with the supplier's Quality Assurance Procedures Manual. A project specific quality plan was prepared to define quality requirements, work activities, deliverables, schedules, and assignment of responsibility. A verification and validation plan was prepared to provide further definition of requirements. The V&V plan implemented was consistent with the industry guidelines on V&V. The V&V plan implemented provided an evaluation of the stages of the software quality assurance process. All V&V reviews were performed in accordance with the plan. Software configuration management procedures were also provided.

6.4.5.3 Software Testing and Verification

The ICCMS software was subjected to extensive design qualification and documentation audits. In addition, an extensive program of equipment qualification testing was completed. Successful completion of the testing and verification demonstrated the acceptability of the ICCMS for use in its intended application. The test configuration, test cases, test procedures, test execution and results of Factory Acceptance Testing were documented in test reports.

6.4.5.3.1 Site Testing and Installation

A technical manual and a site installation procedure were prepared and reviewed to ensure that all elements necessary to install and operate the system were correctly and completely specified. On-site installation and site testing will be done by the utility. All V&V comments and resolutions related to the technical manual and to the site installation procedure were documented.

6.4.5.3.2 V&V Reports

Four interim V&V reports were produced for the ICCMS upgrade project. The first interim report was issued to report on the results of the V&V that was performed during the requirements phase of the project. The second interim report was issued to report on the results of the V&V that was performed during the hardware and software design phase of the project. The third interim report was issued to report on the results

of the V&V that was performed during the implementation, integration and qualification testing phase. The fourth interim report was issued to report on the results of the V&V that was performed during the validation testing phase and the site testing and installation phase. The four interim reports, together with a final report, collectively contained all the V&V documentation produced for the entire project. Resolutions to utility and vendor internal comments were documented during each phase in the interim and final V&V reports.

A complete set of completed V&V checklists and the completed software verification and validation checklist were also documented.

6.4.5.4 Verification of Previously Developed Software

Previously developed software used by the ICCMS was designed by the supplier of the commercial grade computers and a third party. The reviews, audits and V&V of this software was performed by an Owners Group and the supplier. Reports containing the results of the verification and validation were prepared. All open items with respect to the V&V of the software were resolved as follows:

- Sufficient formal testing of the computer in the ICCMS application was completed to offset the lack of test procedures and test reports and to verify correct operating system performance.

- All open error reports were examined to insure that the ICCMS application was not impacted. Details of the review were documented.

- Thread audits were performed on the software. The details of these audits were documented.

The software used in the color LCD touchscreen displays and the Terminal Servers of the ICCMS was subjected to extensive functional testing as part of the ICCMS Factory Acceptance Test (FAT) and reviewed as discussed above. All required functions in all possible operational modes were extensively tested. This testing validated that the components used in the ICCMS would adequately perform their intended functions. In addition, a review of the display software change control procedures indicated that a replacement part received from the device supplier would perform in the same manner as those previously tested and qualified.

6.4.6 Utility Oversight

The Utility Project Engineer was proactive throughout all phases of the project. Weekly project status meetings were typical, and instrumental in establishing communication between the vendor design team, and other cognizant utility disciplines. The project status meetings were used to resolve comments on the project design documents, monitor the progress and process in an ongoing interactive manner, and fine tune the implementation of the requirements to best meet utility needs. For timeliness, vendor specifications and drawings, as well as comments and comment resolution, were transmitted and distributed electronically. This significantly reduced 'copy and distribution' delay times typically associated with large complex documents requiring distribution to multiple disciplines for review, and allowed focus on technical reviews. Hard copy was received under formal transmittal. Comments and their resolution were documented in the V&V report during each phase. The Project Engineer brought utility representatives in the areas of design, operations, maintenance, systems/performance, and human factors (MMI) periodically during each phase. Utility management also participated in pre-FAT demonstrations of the system, and was briefed on project progress. Participation was 'hands-on' in nature, and was instrumental in refining and 'debugging' the final product before FAT.

6.4.7 Utility Surveillance and Audit

In order to satisfy the utility Purchase Order requirements, a surveillance and audit was performed at the ICCMS supplier facility. The surveillance was performed to evaluate implementation of the supplier facility Appendix B Quality Assurance Program relative to the design, fabrication and testing of the replacement ICCMS. The audit covered both the supplier QA and the supplier's dedication of commercial equipment. Two Supplier Surveillance Finding Reports were prepared.

6.4.7.1 Audit Deficiency

Two pseudo-code designs existed for the ICCMS Upgrade software. One design was contained within the Software Design Document (SDD) pseudo-code, and the second was pseudo-code included within the source code listing. There was no objective evidence available to determine which pseudo-code was utilized during the independent review. Actions taken to resolve this deficiency included the following:

- Deleted all pseudo-code included within the source code files. This required a change to the system source files; however, all the executable code remained unchanged. This was verified by running a comparison of the executable software generated from the revised source code with the executable software that underwent

FAT. No differences were found; therefore, no additional testing was required. The output generated by the difference checking utility was documented.

- Performed a more rigorous verification of the source code. This was completed by an independent C programmer doing a detailed comparison of the program listings with the SDD pseudo-code for all modules. No design deficiencies were found.
- Revised the pseudo-code in the SDD to be consistent with the implementation to facilitate software maintenance in the future.

6.4.7.2 Audit Observation

Several revisions to the Requirements Traceability Matrix (RTM) and the Software Configuration Management Plan (SCMP) were suggested. Additionally, this observation identified two instances in which a referenced document was not the latest revision. Actions were taken to resolve this deficiency including the following:

- Updated the RTM to delete non-performance requirements.
- Modified the requirement for remote storage of back-up software to be consistent with Utility contract requirements.
- Required that software tools used in the development, integration, and testing be backed-up and maintained with the source code.
- Updated all documents as necessary to include reference to the latest revision supporting documents.

6.4.8 Project Documentation

The following documents along with many assembly and wiring drawings, and interim and supporting reports, provided the principal documentation for the ICCMS project:

6.4.8.1. Specification for Inadequate Core Cooling Processing and Display System.

6.4.8.2. Specification for Communications of Inadequate Core Cooling System with Plant Computer and Terminal Equipment.

6.4.8.3. Purchase Order

6.4.8.4. Replacement ICCMS Design Document Evaluation.

6.4.8.5. Functional Requirements for the ICCMS

6.4.8.6. Software Requirements Specification for the ICCMS

6.4.8.7. Interface Requirements for the ICCMS

6.4.8.8. Hardware Design Specification for the ICCMS

6.4.8.9. Software Design Description for the ICCMS

6.4.8.10. Final Verification and Validation Report for the ICCMS

6.4.8.11. Factory Acceptance Test Report for the ICCMS

6.4.8.12. Qualification Summary Report for the ICCMS

6.4.8.13. Evaluation of the EMI/RFI Susceptibility of the ICCMS Computer

6.4.8.14. Technical Manual for the ICCMS

6.4.8.15. Site Installation Procedure for the ICCMS

6.4.8.16. Test Report for Point of Installation Electromagnetic Interference (EMI) Mapping of Control Room for ICCMS

6.4.8.17. ICCMS Saturation Margin Uncertainty

6.4.8.18. Software Requirements for ICC Communications

6.4.8.19. Design Change Notice for ICCMS

6.4.8.20. Design Change Report for ICCMS Upgrade

6.4.8.21. Vendor QA audit report

6.4.8.22. Safety Evaluation

These are referred to as Project Document (PD) 6.4.xx in the ICCMS Critical Characteristics Tables 6-7, 8, and 9.

6.4.9 Installation and Lessons Learned

There were some software bugs discovered during installation and testing of the ICCMS. These were minor, but resulted in software changes and reconfiguration after FAT and shipment from the supplier. The changes were made by the supplier on the development system, re-FATed as required, and firmware burned, recertified and shipped to the site for replacement of the old software. Supporting supplemental

documentation (V&V Report, source code, code cert., etc.) were provided. Appropriate site acceptance testing was (re-) performed.

6.4.10 Critical Characteristics

Tables 6-7, 8, and 9 summarize the characteristics of the ICCMS that were evaluated during the ICCMS development and qualification.

Table 6-7.
ICCMS — Physical Critical Characteristics

Physical Critical Characteristic	Acceptance Criteria	Method of Verification
Configuration		Factory Acceptance Tests (FAT) and receipt inspection
• Hardware model numbers	Per Hardware Design Spec (PD* 6.4.8.8)	
• Software revision numbers	Per Software Design Description (PD 6.4.8.9)	
• Cabinet mounting	Per Hardware Design Spec (PD 6.4.8.8)	
Interfaces		FAT and Site Acceptance Tests (SAT)/ utility installation tests
• Electrical power	Per Hardware Design Spec (PD 6.4.8.8)	
• Input signals	Per Interface Requirements Spec (PD 6.4.8.7)	
• Output signals	Per Interface Requirements Spec (PD 6.4.8.7)	
• Contact output	Per Interface Requirements Spec (PD 6.4.8.7)	
• Panel interface (HMI)	Per Hardware Design Spec (PD 6.4.8.8)	

* Project Document; See Section 6.4.8

Table 6-8.
ICCMS — Performance Critical Characteristics

Performance Critical Characteristics	Acceptance Criteria	Method of Verification
Display features	Per Software Requirements Spec (PD 6.4.8.6)	FAT & SAT and PD 6.4.8.10
Heater Control capabilities	Per Functional Requirements Spec (PD 6.4.8.5)	FAT & SAT
Human-machine interface performance, ease of use (including used during operation, configuration, maintenance and troubleshooting)	Per Software Design Description (PD 6.4.8.9)	FAT & SAT
Environmental compatibility: • EMI • Seismic • Temperature • Humidity	Per Hardware Design Spec (PD 6.4.8.8) Per Hardware Design Spec (PD 6.4.8.8) which specifies plant conditions	Third-party test lab reports and PD 6.4.12 (See Section 6.4.4.3 for discussion) Test lab reports and PD 6.4.8.12
Behavior under abnormal/faulted conditions, e.g.: • Loss and re-gain of power • Loss of one or more signal inputs • Input signal over/under range	Per Functional Requirements (PD 6.4.8.5) Per Software Requirements Spec (PD 6.4.8.6)	FAT & SAT

Table 6-9.
ICCMS — Dependability Critical Characteristics

Dependability Critical Characteristic	Acceptance Criteria	Method of Verification
Built-in quality: • Quality of design and manufacture	ICCMS Specification (PD 6.4.8.1 & PD 6.4.8.3)	Vendor QA audit report, PD 6.4.8.21 (See Section 6.4.7 for discussion) and the reviews, audits and reports discussed in Section 6.4.5.
Failure modes and failure management	Per Functional Requirements (PD 6.4.8.5) & Safety Evaluation (PD 6.4.8.22)	FAT and Safety Evaluation Report (PD 6.4.8.22)
Configuration control	Adequate 10 CFR Appendix B program (PD 6.4.8.1)	Vendor QA audit report, PD 6.4.8.21
Problem reporting	Adequate 10 CFR Appendix B program (PD 6.4.8.1)	Vendor QA audit report, PD 6.4.8.21
Reliability	Per Functional Requirements (PD 6.4.8.5) Hardware Design Spec (PD 6.4.8.8)	Review as part of qualification report, PD 6.4.8.12

6.5 MSFIS Upgrade Using PLCs

In this example a number of programmable logic controllers (PLCs), purchased from a commercial vendor, are used in a Main Steam and Feedwater Isolation System (MSFIS) replacement. This illustrates a case similar to the ESFAS example 6.4 of EPRI TR-106439 in which complexity of the commercial digital device (the PLC) and high safety significance of the application (MSFIS) lead to a significantly higher level of effort required to evaluate and dedicate the devices. In general, significant interaction is required among the utility, the designer/integrator of the replacement system, and the commercial vendor in this example. This example is also a case in which multiple copies of the dedicated commercial device are to be used within the system, but the dedication does not need to consider multiple configurations or different functions to be performed by the PLC, as was done in the ESFAS example. In addition, since a manual operation capability is provided, the dedication activities, in particular the examination of the PLC, are not as extensive as were those in the ESFAS example.

6.5.1 Upgrade Bases

A large portion of the system is to be replaced because the MSFIS was identified as a single point failure system that could cause plant trips. The new system design retains

the same basic architecture, but uses PLCs to perform the signal conditioning and logic functions (three channels), and to implement the coincidence logic. The three channels per train redundancy was added in the upgraded system to reduce the likelihood of system failure. A single PLC is used in each of the three channels. Physical separation and electrical isolation are maintained between the two actuation logic trains. However, the same make and model of PLC is used throughout the new system (all channels, both trains). The system includes capability to manually actuate each of the MSFIS functions, using switches that can be operated independent of the PLCs and based on indications that are also independent of the PLCs.

6.5.2 System Overview

The Main Steam and Feedwater Isolation Actuation System (MSFIS) provides outputs to energize or de-energize control solenoids which operate or test the plant's Main Steam Isolation Valves (MSIV) and Feedwater Isolation Valves (FIV). It is a safety system relied upon to help mitigate design basis accidents. The original MSFIS was comprised of electronic circuit modules such as logic modules, input buffer modules, and relay driver modules, interconnected with the power plant sensors to control and alleviate various power plant faults.

The MSFIS is divided into two actuation trains which are independent. Each of the two independent actuation trains monitor system inputs and, by means of logic matrices, energize or de-energize the required solenoids for the appropriate valve operations. Except for the electro-mechanical relays used as the final output devices, the original system circuitry, control and logic, was of solid state design.

Redundant train elements of the MSFIS are electrically and physically isolated from each other so that events (including faults) affecting one element do not affect the others in any way. Independence is provided between redundant train elements to preclude any interaction between trains during maintenance or as a result of train malfunction. Electrical isolation and physical separation are employed to accomplish the required train independence.

6.5.3 System Description

The MSFIS receives discrete (ON/OFF) signals, in the form of contact states, from various systems:

- Main control board
- Valve position switches feedback
- Engineering Safety Features Actuation System (ESFAS) output relays

- Test panel

The MSFIS controls the hydraulic actuators for eight (8) isolation valves, four valves control the Main Steam lines, and four valves control the Feedwater lines. The MSFIS controls four solenoids in each hydraulic actuator, through four contacts of separate actuation relays, installed in the MSFIS cabinet. Overall, each separation group in its dedicated cabinet contains 32 (4x8) actuation relays.

The MSFIS performs logic functions that, based on the inputs from each valve, calculate the required outputs, and control the four actuation relays for each valve. There are two types of control schemes. One controls the "active" side of a hydraulic actuator of the valve. The second controls the "stand-by" side of the hydraulic actuator of the valve. Each control scheme accepts inputs from the control panel or ESFAS and feedback from valve switches, and controls the four actuation relays, that in turn control the four solenoids. The difference between the "active" and "stand-by" control scheme is the inputs to each of them.

The MSFIS is composed of two Separation Groups (A and B). Each Separation Group is installed in a separate cabinet, controlling the same eight valves. To control a valve, four actuation relays from one Separation Group are connected to the "active" side of the hydraulic actuator of a specific valve, and four actuation relays from the second Separation Group are connected to the "stand-by" side of the hydraulic actuator of the same valve.

6.5.4 Replacement System Hardware Description

A general block diagram of the MSFIS is presented in Figure 6.3. From a hardware point of view, the system is comprised of two identical cabinets, one contains Separation Group A and the second contains Separation Group B. This configuration provides the separation and isolation between the two trains. The cabinets for each Separation Group are identical and the following description concentrates mainly on one cabinet, since the second cabinet is identical.

Each cabinet (separation group) contains the following subsystems:

- Programmable Logic Controllers (PLC)
  - — Input modules to read the input signals
  - — Digital processor to implement the logic
  - — Output modules to control the output devices (actuation relays)
  - — 125 VDC power supply to operate the PLC

- Interposing relays (actuation relays) to control the solenoids
- 125/48VDC converter to provide voltage for energizing actuation relays, and wetting voltage for input signal contacts
- Test Panel

48 VDC from the power supply provides wetting voltage for the input contacts. The inputs from the field contacts are sensed by the input modules of the Programmable Logic Controller (PLC). These modules sense the voltage, convert it into a '0' or '1' bit, and send it to the PLC processor. Based on the inputs, the PLC processor implements the control logic. The processor controls the output modules of the PLC. These modules contain relays that control the 48 VDC to the coil of each of the actuation relays. The actuation relays are the existing relays currently installed in the system.

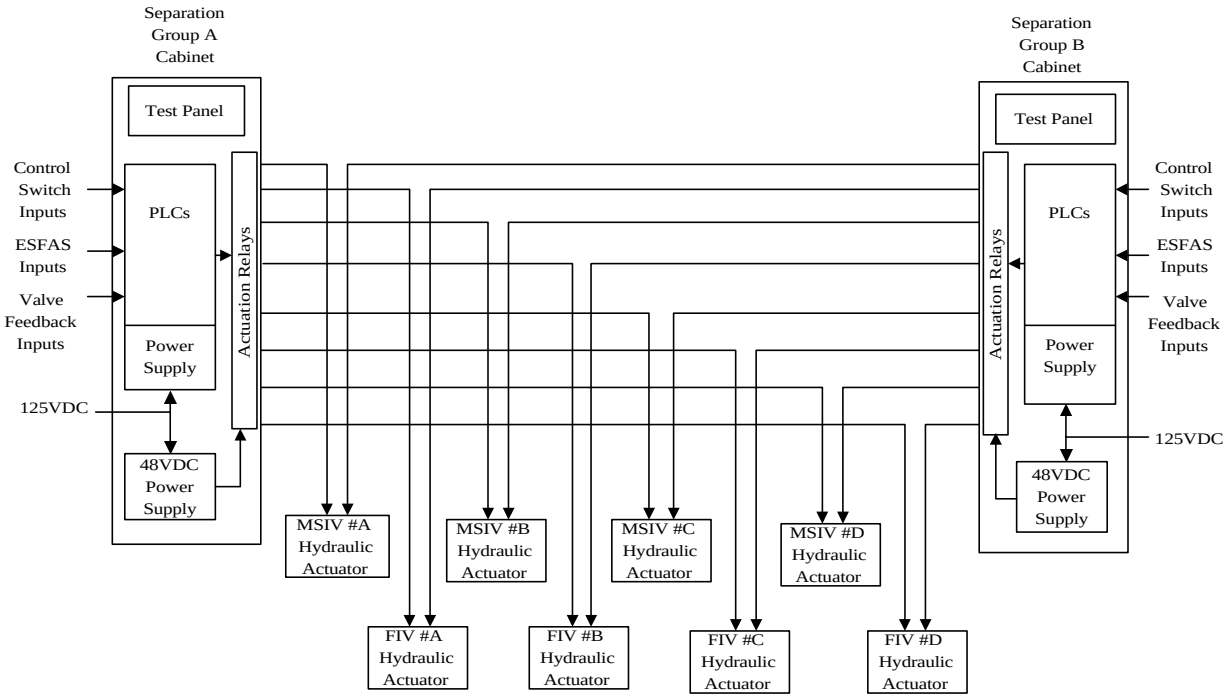


Figure 6-3.
MSFIS General Block Diagram

The valve control logic is implemented using a redundant three (3) channel architecture. These are referred to herein as *logic channels* to distinguish them from the two trains which comprise the Group A and B MSFIS actuation trains. Each logic channel consists of identical and interchangeable components, including a PLC and associated I/O modules, and the modules for each channel shall be contained within a single rack except for the power supply. The same PLC modules are used for all PLC functions. All inputs are read by each logic channel. Output coincidence for each output is

obtained by cross-connecting two (2) contacts from each logic channel, such that 2 out of 3 coincidence is obtained. Therefore, the software in each of the three logic channels is identical. Two basic modes of operation are provided for each valve, normal and test.

Each cabinet also contains a Test Panel mounted on the front of the cabinet. It contains switches and lights to permit complete testing of each valve actuation train and logic channel.

6.5.5 System Design and Dedication

The MSFIS replacement was designed and developed by the supplier utilizing Programmable Logic Controllers (PLCs) which perform the same logic as the original system design. The PLCs use firmware of the PLC family of controllers and ladder logic software to develop the application software. The supplier is a 10 CFR 50 Appendix B supplier and is on the utility Quality Supplier List. The supplier purchased the MSFIS equipment and provided commercial grade dedication for its safety related functions. The supplier was successfully audited by NUPIC, and the utility and a contractor performed a critical design review of the MSFIS design at the supplier and found no significant concerns.

The system is comprised of triple redundant logic consisting of three logic channels in two different trains or separation groups. The triple redundant logic provide the MSFIS equipment with a 2 out of 3 voting scheme. The output module contacts for each logic channel are normally open and close to trip. The 2 out of 3 voting scheme solves the problem of a 1 out of 2 nuisance actuation. To trigger an actuation, two logic channels (i.e., A-B, A-C, or B-C) per train trip to trigger the actuation and energize the actuation relays. Each train of MSFIS contains 3 PLCs, one for each logic channel. This logic design requires coincidence testing to ensure each set of combinations can produce an actuation. The 2 out of 3 logic design increases plant reliability and availability. A single failure cannot trigger a false actuation, nor prevent a true actuation from occurring. If one logic channel fails, the affected train reverts to a 2 out of 2 logic. If a PLC channel failure occurs, a Channel Failure light will energize on the MSFIS test panel and the Main Control Board annunciation of the Channel Failure will occur. A Probability Risk Assessment (PRA) was performed by the utility which evaluated the logic scheme.

The ESFAS and the Main Control Board (MCB) hand switches still input to the MSFIS cabinets. The existing actuation output relays, input terminal boards, and output terminal boards are utilized. The man-machine interface for operators and maintenance technicians is similar to the original configuration, except that local PLC fault indication and coincidence logic test functions are provided. The coincidence logic test functions are accomplished on the MSFIS test panel where each combination of input signals can be tested.

Each MSFIS cabinet consists of three PLCs, external watchdog timers, interposing (actuation) relays, a 125/48 VDC converter to provide voltage to energize the actuation relays and energizing voltage for input signal contacts, and a test panel. The test panel contains indicators and controls. Each PLC is comprised of input modules which read the input signals, a digital processor to implement the logic, output modules to control the output devices (actuation relays and status indicators), and a 125/5 VDC power supply to operate the PLC.

Each MSFIS cabinet contains toggle switches for each of the four MSIVs and four FIVs and the switches are located on the Emergency Override Panel. With a Feedwater Isolation Signal present, the FIV toggle switches (NORMAL and BYPASS positions) provide a bypass to the Feedwater Isolation Signal to allow opening of the FIVs and the operation of the Main Feed Pumps to supply feed flow to the Steam Generators. This bypass annunciates on the ESF Status Panels for each FIV valve. The toggle switches (NORMAL and FULL CLOSED positions) for the MSIVs are used to provide a diverse means to manually fast close the MSIVs in case of a common mode software failure coincident with an accident requiring an MSIV closure.

6.5.5.1 MSFIS Software

The software was designed in accordance with ANI/IEEE-ANS-7-4.3.2-1993, "Criteria for Programmable Digital Computer System Software in Safety-Related Systems of Nuclear Power Plants," and ANSI/IEEE 1012-1986, "IEEE Standard for Software Verification and Validation Plans".

The application software was developed by the supplier utilizing PLCs and third party programming software. Using structured design principles, the top level design of the MSFIS software was intended to be simple and straight forward. Interrupts (an event that would cause the normal program flowpath to be interrupted) were not used in the MSFIS software and all programs are single task (i.e., no multi-tasking - a program structure that performs multiple tasks simultaneously). The software was designed with a modular structure which is beneficial for testing and verification.

The software was developed and organized to consist of several software programs as follows: Main, Initialize, Run, Input, Valve Logic, Output, Self Test, and Fault. The main program calls the Initialize and Run programs upon powerup of MSFIS. First, the Initialize program will reset all the timers, set system outputs to 0, and have the Self Test program check for minor faults before processing begins. Next, the Run program "reads" the inputs, executes the valve logic, and "writes" to the outputs. If any of the programs generate a fault, the Fault program will energize the "Chan Fail" light. All application software reside in Erasable Programmable Read Only Memory (EPROM).

Verification, including a code verification walkthrough, was performed by supplier personnel who were independent of the design processes. Implementation of the

Software Verification and Validation (V&V) Plan was the responsibility of the supplier Quality Assurance group, which is independent of the project development group and reports directly to the supplier's President. The V&V engineer performed and directed the performance of the V&V activities for the project. The Walkthrough Verification Report documents this review.

The V&V of the MSFIS replacement was a structured method that included the supplier V&V Plan, the review process and policies for technical reviews, software and hardware testing of normal and abnormal events, and an independent stage-to-stage verification of each phase of the software life cycle per IEEE 1012-1986. The supplier's software life cycle followed the "waterfall model".

The V&V of the MSFIS hardware and software started with the utility specification and followed two paths until integration testing occurred at the end of the process. Initially, a System Requirements Document (SRD) was written and reviewed with the utility to ensure all the requirements of the utility specifications were met. Further details of the software requirements and input/output requirements were specified in the Software and Hardware Requirements Specifications (SRS & HRS). Next, the specific subroutines and parameters were defined and hardware drawings were completed with the development of the Software and Hardware Design Documents (SDD & HDD). At this point, a joint review by the utility and the supplier provided a line-by-line verification of requirements.

After the software was coded into the ladder logic diagrams (LLDs), the code was tested by a walk-through phase to verify compliance with the Software Design Document (SDD). The walkthrough verification provided a line-by-line review of the code to ensure the requirements of the SDD were correctly implemented, and that no unintended functions were present. Software nonconformance reports were generated to document and resolve any errors which were reported in the Walkthrough Verification Report.

The software was then Module tested with Software Unit Tests (SUTs). Modules are well-defined software units that are independently testable with a predictable behavior. The SUTs tested each module under all possible combinations of inputs and system parameters. Test procedures were developed for each module and the test results were documented in the Software Unit Test Report. Once the SUTs are performed and verified, the Software/Hardware Acceptance Test (SHAT) validated that all individual modules would communicate correctly and verified the integration of the hardware and software. Before the application software was loaded on the PLC, a Ladder Logic Report was generated, which was the conversion of the binary ladder logic data file to a human readable text format. The application software was downloaded into the PLC processor as a binary file. Also, the Programmable Read Only Memory (PROM) contents can be stored in HEX code prior to loading the EPROM, which can be compared bit-by-bit after loading.

The SHAT was performed on a pre-production unit that was driven by a PC to emulate system inputs. The unit was loaded with the application software and tested to verify functions specified in the design documents. Finally, the application software was loaded onto the production units and tested with the hardware during a Factory Acceptance Test (FAT). The production units were shipped to the utility plant and installed by site personnel. Following installation, a Site Acceptance Test (SAT), was performed to verify and validate proper operation and complete surveillance procedures.

The application software was supplied in EPROM. The software code and documentation are kept under configuration management control by the supplier. A design modification will be required to make software changes. Any changes required will be made after a review to determine the impact of the change on other components and the need for re-testing or modification of test procedures. All modified code will be subjected to the Verification and Validation process as described above.

6.5.5.2 Equipment Qualification

The MSFIS was designed to withstand the effects of natural phenomenon and was qualified to operate in normal and post accident conditions. The system was qualified to perform its intended safety function under the environmental conditions of temperature and humidity, seismic, electromagnetic and radio frequency interference (EMI & RFI), and radiation.

The supplier reviewed the equipment specifications for the equipment for compliance with IEEE 323-1974. The current MSFIS equipment is located in a mild environment and designed to operate over a temperature range of 60 to 120°F in a relative humidity between 30% to 70% without loss of protective function. The equipment was specified to operate over a temperature range of 0 to 140°F in a relative humidity range of 5% to 95%. In addition, the MSFIS equipment was qualified to 1000 rads. Therefore, the new equipment is qualified for an environment that exceeds the existing design requirements.

The heat load of the new equipment is less than the existing equipment and will not challenge the cabinet or room temperature profiles.

The MSFIS cabinets will remain in place and utilize the existing terminal boards and actuation relays. Only the electronic circuit cards, card frames, power supplies, and test panel were removed. The MSFIS components were subjected to multi-axis/frequency inputs in accordance with IEEE 344-1975, to a plant generic seismic spectra profile. The components were seismically tested with software running. The existing cabinets were previously qualified prior to installation and seismic analysis demonstrated the qualification of the new equipment installed in the existing cabinets.

The supplier qualified the MSFIS replacement equipment in accordance with EPRI TR-102323-EMI guideline (IEC - International Standard 801 Parts 2-6 and MIL-STD-461 EMI Susceptibility and Emission Requirements) to meet the EPRI EMI limiting practices. The emission levels established for the utility plant were enveloped by the testing performed by EPRI. The emission levels were established in the EPRI guide per the emission envelopes of CE (Conducted Emission) 102 and RE (Radiated Emission) 102. The susceptibility levels were established in the EPRI guide per IEC 801-4 (Fast Transients), IEC 801-5 (Surge Tests), CS (Conducted Susceptibility) 101 - Low Frequency, CS 114 - Hi Frequency, RS (Radiated Susceptibility) 103 - Electric Fields, and IEC 801-2 (Electrostatic Discharge). The components were EMI/RFI tested at a test lab.

The cabinets are located in the back of the Main Control Room next to other electronic instrumentation panels. The surrounding rooms are the upper and lower cable spreading rooms. Use of radio transceivers is prohibited in this area. This restriction limits high frequency radiated emissions concerns. Any low frequency emissions will be attenuated by the small wavelength the cabinet openings present to low frequency signals which require a rather large wavelength in order to propagate.

Electrostatic discharge (ESD) can cause damage to electronic devices and has been known to cause lock-ups on digital equipment if a large enough discharge occurs. Maintenance on the MSFIS requires prior installation of ESD grounding straps.

6.5.5.3 Interaction Between 1E And Non 1E Equipment

The only interaction between the MSFIS and non IE equipment is the connection to the plant annunciator system. These outputs are isolated by use of optical isolation devices in the Plant Annunciator Isolator Cabinet. These isolators were installed as part of the original plant design.

6.5.5.4 Reliability

The MSFIS replacement equipment has a two out of three logic design that assures increased reliability over the original single-channel logic design. The equipment, processors and input/output modules have sufficient field operating experience to estimate the MTBF (calculated at $> 10^6$ Hrs). The original system had a lower reliability (calculated at $> 10^5$ Hrs).

The design of the software received an extensive V&V process by the supplier, per IEEE 1012, as previously stated. The supplier had provided digital upgrade equipment and similar PLC software for other nuclear plant applications. Also, the supplier had experience with an established software life cycle process which conforms to IEEE 7-4.3.2-1993. Thus, as a result of utilizing an extensive development process, the supplier produced a software product of high quality and reliability.

A common mode software failure could exist if both trains of PLCs have a simultaneous software malfunction and/or fault. This potential failure would prevent the operator from manually fast closing (FC) the FIVs or MSIVs from the Main Control Board. Diversity is one method of addressing this concern. If adequate diversity exists or can be added to the design, then computer/PLC diversity is not necessary.

A diverse means to operate the MSIVs was not available. Therefore, an MSIV Fast Closure toggle switch for each valve to allow manual operator action in the event of a common mode software failure coincident with an accident requiring an MSIV closure was added to the MSIV train cabinet. Control Room indicators (e.g., steamline pressure, containment pressure, SG level) are available to permit manual mitigation of the accidents in the unlikely event of a common mode failure. Based upon the high quality established throughout the equipment design process, the possibility of a common mode failure is reduced to a very low probability. Thus, in the event of a common mode software failure, sufficient indication diverse from the MSFIS and procedural guidance from operating procedures exist for the operator to take manual actions to mitigate transients.

A Failure Modes and Effects Analysis was performed by the supplier. The results indicated that no single failure would produce the loss of a protective function. The MSFIS equipment performs self-tests at the end of each scan cycle. If any failures are diagnosed, a channel failure will occur and be annunciated. The PLCs have an internal watchdog timer (WDT) which will time-out and produce a channel failure if the processor is caught in a loop. However, if the processor halts due to a software failure, the internal WDT may not time out, thus, and external watchdog timer was added to time-out and alert the operator with a channel failure.

6.5.5.5 Testing

Factory Acceptance Testing (FAT) was performed by the supplier. The testing verified that the MSFIS equipment met the accuracy and functional requirements specified in the utility's design specification. Utility personnel witnessed portions of the testing and reviewed deficiency reports produced.

The utility in conjunction with the supplier performed Site Acceptance Testing (SAT) once the equipment was installed.

6.5.5.6 Operating History

The PLC selected was introduced in 1988 and at the time of the upgrade had exceeded 25,000 units in use. Since these units are provided commercially, the supplier commercially dedicated the PLC for the MSFIS application at the utility plant in accordance with EPRI Guideline NP 5652. The supplier performed a receipt inspection

of the hardware and checked it for functional attributes and critical characteristics. The software provided by the PLC vendor was tested by the supplier to check the instructions and verify that no unintended functions are present. A ladder logic program was written which tested each instruction in all modes, checked the results against expectation and set a bit if the test fails. All status bits were checked for failure at the end of the test. Similar testing was performed for new versions of software. The third party software, which was utilized to develop the source code offline, was also commercially dedicated.

When the PLC vendor revises their equipment or issues product safety alerts, they notify their distributors and also notify their purchasers. The supplier will perform a hazards analysis for the change, if required. This analysis ensures updates are transmitted to the customer when changes occur. The third party software vendor transmits their revisions in a similar manner. The PLC vendor will be added to the utility's Vendor Equipment Technical Information Program.

The PLC vendor maintains design control of their product lines. Also, the PLC vendor identifies the product need, reviews changes, and assigns a design review committee for implementation. Functional confirmation testing is performed on each product line. The PLC vendor maintains a qualified supplier list.

Hardware and software suppliers were added to the utility's approved supplier list after a survey of the suppliers' quality process was completed. The survey focused on the suppliers' quality assurance manual, and their software life cycle processes. Each year, questionnaires are sent to the suppliers to provide management and/or process changes which might effect quality. Class 1E suppliers are surveyed every three years.

A PLC vendor survey was completed by the supplier to thread through the development and manufacturing process of the PLC units. The results were acceptable, with an action to assure correct identification of PROM firmware revisions. As a result, a PROM reader was purchased and a receipt inspection procedure was established to "read" the PROM and perform a checksum. The replacement checksum is compared to the current PROM's checksum.

The third party software vendor was also surveyed by the supplier to verify their process for ladder logic editing, on-line communications for down loading, on-line editing, and PLC monitoring. The applications engineers act as verifiers and contact customers if any software problems arise that could affect them.

6.5.5.7 Critical Digital Review (CDR)

A critical digital review of the system design, PLCs, and software was also performed to support the dedication. The CDR was performed by an independent contractor. As a result of the review, an external watchdog timer was added to the design.

6.5.5.8 Training And Procedures

A number of procedures were revised as a result of this modification. The affected procedures include surveillance, annunciator response, and operator aids.

The supplier provided the operation and maintenance manual for the new system.

Training was provided for the Instrumentation and Control, Engineering, and Operations Departments.

6.5.5.9 Safety Evaluation

A safety evaluation was performed to support the MSFIS modification. It concluded that the change constituted an Unreviewed Safety Question and NRC approval was needed for the change. Technical Specification changes were also required for the upgrade.

6.5.6 Utility/Supplier Interaction

Throughout the design process, the utility interfaced with the supplier to ensure the plant specific design requirements were met. The utility participated in a conceptual design review and interim design review, and participated in a Factory Acceptance Test (FAT) at the supplier. The supplier visited utility plant to walkdown specific details associated with the design. Various comments and discrepancies were generated by the supplier throughout the design and testing with subsequent resolution by both parties, as required.

6.5.7 Identification and Verification of Critical Characteristics

Critical characteristics were identified based on the safety-related functions of the PLC. Examples of the critical characteristics identified are shown in Tables 6-10, 11, and 12. Acceptance criteria and verification methods are also listed in the table.

6.5.8 Documentation

A dedication package was prepared that documents the critical characteristics, verification methods employed, and the basis for the judgments made in accepting the PLC for the MSFIS application.

The PLCs were entered into the utility's tracking system for dedicated commercial equipment. This included placing the firmware, the software tool used for PLC configuration and programming, the application programs, and the hardware under configuration control.

Table 6-10.
MSFIS Programmable Logic Controller — Physical Critical Characteristics

Physical Critical Characteristic	Acceptance Criteria	Method of Verification
Configuration • Model number • Software revision number • Case type, dimensions and mounting	 Vendor model # Vendor software revision # Case type, dimensions and mounting per utility specification	Receipt inspection
Interfaces • Electrical power • Grounding and shield termination provisions • Number and type of inputs • Input impedance (with and without power) • Number and type of outputs • Output characteristics (e.g., current drive, sink capability) • Programmer (software configuration) interface • Front panel interface (HMI)	Per utility specification	Receipt inspection and testing for each unit received. Some characteristics are verified by special testing on one unit (e.g., test to verify maximum output current capability as part of design verification) along with review of vendor design information and vendor testing.

Table 6-11.
MSFIS Programmable Logic Controller — Performance Critical Characteristics

Performance Critical Characteristic	Acceptance Criteria	Method of Verification
Signal conditioning and logic functions: • Input signal filtering including anti-alias filters • Combinatorial logic functions required • Timing and latching functions • Blocking and inhibiting functions • Output isolation	Per utility specification	Verified through a combination of: • Review of PLC design including input module filters, anti-alias protection, implementation of required logic functions • Review of documented vendor testing for these features • Tests performed by the supplier of the configured PLCs, verifying proper functionality (tests verify application programming as well as PLC function) • Site acceptance testing for the integrated system
Response time including: • Time for logic units to produce actuation output in response to appropriate combination of valid inputs	Per utility specification, based on required overall response time as used in safety analysis	Review of PLC system design, including input sample rate, processing time, and total lifecycle time including output propagation and covering worst-case combination of times for PLC from sensing to actuation. Final verification via testing of integrated system.
• Human-machine interface performance and ease of use, including use during: • Operation (e.g., indications provided for status, fault indication, etc.) • Configuration (ease of use, protection against mis-configuration, security features, etc.) • Maintenance and troubleshooting	Per utility specification, covering operational requirements, configuration capabilities, maintenance and troubleshooting, and general human factors criteria.	Detailed review of design and operation of the PLC during commercial grade survey, special testing by supplier, and human factors evaluation by utility engineering and operations.

Performance Critical Characteristic	Acceptance Criteria	Method of Verification
(e.g., diagnostic information provided, clarity of information, etc.		
Environmental compatibility:		
• EMI	Per utility specification (e.g., using EPRI TR-102323)	Vendor testing, detailed review of hardware design and EMI protection features, laboratory testing of PLC susceptibility and emissions in configurations that mimic as close as possible the installed configurations, and post-installation testing. This is coupled with specific practices followed in installation and wiring of power and signal cables and in grounding configuration for the MSFIS application.
• Seismic	Per response spectra chosen to envelop application location	Third-party laboratory testing plus review of hardware and mounting design, including assembly and positive locking of plug-in components.
• Temperature	Per utility specification	Third-party laboratory testing, plus review of reliability analysis assumptions regarding temperature.
Behavior under abnormal/faulted conditions, e.g.: • Loss of power to one or more modules • Failure of an I/O module • Loss of one or more signal inputs • Short and open circuit of input or output • Input signal over/under range	Per specific requirements regarding fail-safe conditions of the controller.	Review of vendor testing, detailed review of PLC design and hardware/ software architecture during commercial grade survey, failure analysis including FMEA for the controller, plus special tests performed by the utility to examine behavior under expected abnormal/faulted conditions, verifying safe response of PLC.

Table 6-12.
MSFIS Programmable Logic Controller — Dependability Critical CharacteristicsSFIS

Dependability Critical Characteristic	Acceptance Criteria	Method of Verification
Built-in quality • Quality of design and manufacture	Vendor maintains a QA program that generally is in compliance with a recognized standard (e.g., ISO 9000). QA program addresses key areas including, as a minimum: • QA staff and organization definition • QA plans and procedures Specific software QA procedures (e.g., ISO 9000-3) Evidence that the QA program was applied in the production of the procured item(s) hardware and recently developed software. Vendor presently follows a digital system/software development process that includes: • Software development plan and organization • Documented design requirements, including software requirements • Requirements traceability • Documented software design descriptions • Documented V&V plan • Validation test reporting Documented product operating history showing product stability, reliability, and freedom from critical software-related errors or failures in similar applications. The items listed above, taken together, demonstrate adequate quality of the PLCs.	Commercial grade survey, including: • Review of vendor QA program against relevant standards • Review of vendor procedures and practices for digital system/software development, V&V, and testing for each module/unit to be procured, and how these processes have evolved. • Thread audit to check actual practices for QA and software development and control. • Check of degree to which QA program and software development process were applied in the design and production of the PLCs procured • Review of PLC design, software architecture including task management, and implementation of diagnostics and error detection • Review of software coding procedures used in development • Samples of the software code reviewed to check adherence to established coding practices and to support the thread audit. • Review of operating experience with the specific controller modules and configuration to be procured. • Review of types of applications, physical environment, software features used, types of application programs. • Review of vendor's data on problems and error rates.

7

REFERENCES

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

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

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

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

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

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

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

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

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

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

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

12. EPRI TR-101984, "Application of a Cost-Benefit Analysis Methodology to Nuclear I&C System Upgrades," 1992.

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

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

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

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

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

18. EPRI TR-104913, "Proceedings: Distributed Digital Systems, Plant Process Computers, and Networks," 1995.

19. EPRI TR-104963, "Instrumentation and Control Upgrade Evaluation Methodology," Vols 1&2, 1996.

20. EPRI TR-106029, "Instrumentation and Control System Maintenance Plan Methodology," Vols. 1&2, 1996.

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

22. IEC 880-1986, "Software for Computers in the Safety Systems of Nuclear Power Stations."

23. IEC 1226, "Nuclear Power Plants ◊ Instrumentation and Control Systems Important for Safety - Classification," 1993.

24. IEC 1508, "Functional Safety: Safety-Related Systems. Part 1: General Requirements (Draft)," 1995.

25. IEEE 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

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

27. ISA-S84.01-1996, "Application of Safety Instrumented Systems for the Process Industries," 1996.

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

29. National Research Council, "Digital Instrumentation and Control Systems in Nuclear Power Plants," National Academy Press, 1997.

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

31. NRC Generic Letter 91-05, "Licensee Commercial-Grade Procurement and Dedication Programs," 1991.

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

33. NRC Inspection Procedure # 38703, "Commercial Grade Dedication," 1996.

34. NUREG/CR-5930, NIST 500-204, "High Integrity Software Standards and Guidelines," 1992.

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

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

37. NUREG 0737 Supplement 1, "Clarification of TMI Action Plan Requirements ✍ Requirements for Emergency Response Capability," 1983.

38. NUREG 0800, Standard Review Plan Chapter 7, "Instrumentation and Control," Rev. 4, 1997.

39. Title 10 of the Code of Federal Regulations, Part 21, "Reporting of Defects and Noncompliance," 1995.

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

8

INDEX

A

CRITICAL DIGITAL REVIEWS

This appendix describes one method that has been used successfully in performing a critical review for digital equipment. Referred to as a Critical Digital Review (CDR), this method has been applied successfully both for commercial equipment and equipment developed under a 10 CFR 50 Appendix B program. It is a focused, technical review of the digital product and the vendor, performed primarily at the vendor's facility.

Detailed "how-to" guidance is given, along with examples and anecdotes that help illustrate the method. See Section 5.4 in the main body of this report for more information on critical design reviews and how these relate to dedication of commercial digital equipment.

TABLE OF CONTENTS

1 Introduction to Critical Digital Reviews

For decades engineers have applied processes in pursuit of assurance that the requirements for a critical system are clearly and thoroughly defined, and that the actual system will function according to those requirements. Engineers are prepared to specify hardware requirements, and to critically inspect, review, and test *hardware* components, subsystems, and systems.

With microprocessor and computer based systems (digital systems), however, there is an added *software* dimension, where established hardware-oriented processes fall short. A digital system cannot be adequately inspected, reviewed, or tested with the same techniques used for pumps, valves, piping, and bolts, or even with the same techniques used for analog electronic components.

Unfortunately, there are no uniformly practiced digital design methods in which the nuclear utility engineer can find easy assurance. While there are multitudes of standards, procedures, and methods for developing software, none has been shown to guarantee safe and/or reliable software. Furthermore, there is wide variation of opinion among commercial suppliers about the cost/benefit justification of formal software quality assurance methods.

The same lack of uniformly practiced methodology exists for software testing as well. It is generally not feasible to perform exhaustive testing where software modules are subjected to every possible situation that may be encountered in service. Even if such comprehensive testing were possible for normal circumstances, physical events can produce random memory errors, which essentially modify the program in an unpredictable way.

An excellent source of further reading on the nature of risk with digital technology is the book *Safeware* by Leveson[1].

So what additional steps can a nuclear utility engineer take to gain assurance that requirements for a *digital* system are thoroughly specified and that the actual system will function according to those specifications? Nothing can be done to gain complete (100% guaranteed defect-free) assurance. However, there are methods that can be used to provide an adequate level of assurance. The main part of this report, coupled with the higher-level guideline TR-106439, describes how a combination of methods and techniques can be used to provide adequate assurance when commercial digital equipment is applied. Typically, reaching an adequate level of assurance requires a combination of testing, review of operating history, knowledge of the vendor's system

[1] Leveson, Nancy G., *Safeware: System Safety and Computers*, Addison Wesley, 1995 (ISBN 0-201-11972-2)

development and quality assurance practices, and a critical review of the design of the digital system.

This document outlines one method for performing a critical design review of a digital system or device. The method is a focused technical review, called a *critical digital review* (CDR), which investigates one of the key concerns when evaluating digital systems: the potential for unforeseen events to occur in service due to the digital system design or its application, configuration or documentation. Often, a CDR can be performed in conjunction with a commercial grade vendor survey.

1.1 Objectives and Organization of this Appendix

The purpose of this appendix is to provide practical guidance to nuclear utility engineers on how to conduct a Critical Digital Review. After reading this document, the engineer should know what to expect from a CDR and how to organize and prepare for conducting a CDR, whether it is performed separately or in conjunction with a vendor survey or audit.

This document is divided into three sections. This section provides a background from which to view the Critical Digital Review (i.e., it answers the "why" question). The second section provides guidance for actually performing the review (i.e., it answers the "how" question). The final section discusses the post-review activities.

Throughout this document, stand-alone figures and text boxes accompany the main body of the text to provide specific examples, sample questions, and clarifications. There is no "cookbook" for conducting critical digital reviews. A CDR is at least in part a discovery process, in which information is uncovered and the answers to one set of questions may lead to pursuing a new line of questions or reviews. The stand-alone figures and boxes provide examples and anecdotal material to convey an understanding of the various paths a CDR might take. The lists that are given are not all-inclusive.

1.2 Critical Digital Review Basics

What is a Critical Digital Review?

Simply stated, a Critical Digital Review is a focused technical review applied to a specific digital systems project to investigate the potential for unforeseen events, and to recommend mitigation strategies. "Unforeseen events" are not limited to the actual operation of the physical system. For example, the lack of proper documentation to correctly configure a component required for continued operation on a back shift — when the vendor may not have support available — may be an unforeseen event.

The deliverables of a CDR are: 1) a list of recommended action items outlining potential problems and mitigation alternatives, 2) descriptions of the digital system and the development/maintenance process (including documentation), and 3) detailed discussions of any especially important technical details. The deliverables must be written so that the project team can apply the gained knowledge to their specific project.

What is "Astute Technical Perspective"?

A CDR utilizes a strategy where the first objective is to penetrate the technical shell of the digital portion of the system, as illustrated in Figure A-1. The goal of this penetration is to gain a detailed knowledge of the core "technical architecture." The core technical architecture is then used as a basis for questioning all issues relevant to requirements, expectations, and the potential for unforeseen events.

Penetrating to the core technical architecture requires an "astute technical perspective." In short, astute technical perspective means sharp technical expertise tempered by a pragmatic sense of what level of detail is important in the discussion of vendor processes, system architecture, and unforeseen behavior.

Technical expertise in digital hardware, software, and real-time systems is certainly required of the review team. The team must be able guide the discussions based on potential consequences to the plant system. From the beginning, the team must actively pursue the technical core and avoid philosophical discussions over internal implementation that do not impact system behavior important for this project.

What is the Relationship Between a Critical Digital Review and an Audit or Survey?

The CDR by itself does not constitute an audit or a survey. The CDR is not a substitute for an audit or survey. There is, however, some overlap in activities, objectives, and results. Utilities may find that the CDR, or the results of the CDR may be used as input to, in conjunction with, or as an integral part of an audit or survey. Combining these activities may be the most efficient and cost-effective approach for both the utility and the vendor.

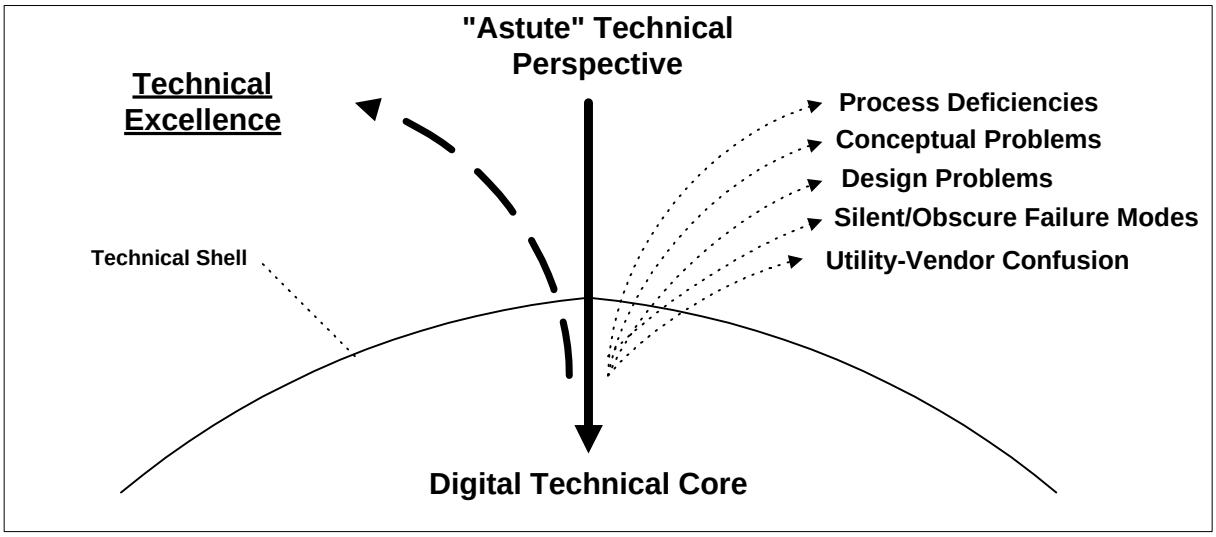


Figure A-1. CDR Penetrates to Core Architecture

Why Perform a Critical Digital Review?

Digital technology, while providing a vast array of benefits, can also exhibit obscure behavior and unique failure modes. Even for a digital upgrade that is intended to provide exactly the same external functionality as its analog predecessor, there may be the potential for unforeseen behavior.

A good question to ask is: "Can an undetected or unrecognized failure in this system cause or enable significant consequences?" If the answer is "no," then an audit or survey of vendor practices may be sufficient. If the answer is "yes," a CDR can help identify unforeseen events, and potential mitigation strategies.

Performing a CDR early in the design process can also:

- clarify both scope and requirements for utilities and vendors
- identify options and/or alternatives prior to detailed design
- identify non-suitable equipment
- identify potential risks
- identify potential mitigation strategies
- promote reasonable vendor/customer expectations

Each of these benefits has the potential to reduce overall project, and lifecycle, cost.

Potential for Unforeseen Events

By "unforeseen event" we mean an event or situation that is a surprise to the project team. The event may be associated with unforeseen behavior of the system, or with an unforeseen confusing or difficult situation. It may be a surprise to the vendor as well as the user. However, sometimes potential behavior is known by the designers but not recognized as significant or potentially undesirable for a particular user application. Listed below are some of the questions a CDR attempts to answer to find potential unforeseen events.

Are the utility and supplier on the same page about project requirements and expectations, and about foreseeable behavior of the device? One could say that this is precisely the CDR objective -- to get digital equipment designers, programmers, and project team members on the same page to talk about system behavior as it relates to this application. It takes an astute technical perspective to facilitate this process.

Are there design problems (questionable decisions) that open the door to unforeseen failure modes? In some cases, potential for behavior unforeseen by the project team is discovered in tradeoff decisions the designers made about the digital system. The decisions may have been acceptable for some applications, but questionable for this project.

Are there failure modes whose behavior may lead to inaction (or unfortunate actions) by people? Digital designers and programmers often do not go far enough in considering the impact of design issues and decisions. That is, they may not take each failure mode and consider how operators are likely to interpret and react to the system behavior.

Are there conceptual problems (oversights) in the design or testing plans? Conceptual oversights in the design or test plans can lead to behavior which is unforeseen by the designers.

Are there weaknesses in the supplier processes that give concern about the level of discipline and teamwork in the design and programming effort? If questioning during a CDR reveals genuine teamwork and uncovers no conceptual problems, then concern by the CDR team about conceptual problems is largely put to rest. On the other hand, if there was clearly no teamwork in developing the concepts and design, this is cause for concern even if no specific conceptual problems were found.

Are there weaknesses in the supplier processes that increase concern about software bugs and product support? A thorough review of the software code is beyond the scope of a CDR. Only through evidence of discipline and teamwork in software development and support processes can the CDR team gain confidence that bugs will be few after testing, and that they will decrease over time with no surprises in future releases or replacements.

Is there sufficient documentation for efficient and correct component replacements? It may happen that if a system fails and components must be replaced, there is confusion about the correct settings of important jumpers, switches, parameters, etc. The CDR looks for documentation sufficient to avoid this type of confusion.

Are known problems communicated to the people responsible for maintaining the system? Sometimes unforeseen events arise because the people responsible for maintaining the system have not been informed of known problems.

Unforeseen Behavior Examples

Here are some examples of potential unforeseen events. Some of these were discovered the hard way, through unforeseen significant events. Others were discovered during reviews prior to any operational event occurring. A few are taken from similar systems found in the petrochemical industry.

In a radiation monitor, raw data was "live", but calculated values were "frozen". *Design problem:* The watchdog timer was not designed to assert a failure if any critical task gets "locked out". Lockout can happen if some situation causes high-priority tasks to execute more often than usual, or if high-priority tasks require more time than usual to execute. Lockout causes calculated variables to remain at their last calculated values.

In a digital feedwater system: Redundant computers exercise control, with each loop going through a commercial single-loop controller. One computer is active and the other tracks it, with a switching system used to route the active computer through the controller. *Obscure behavior*: A failure (run-time error) in the single-loop controller caused feedwater valves to drift (sample and hold circuits no longer refreshed), with no way for operators to assume manual control.

In the same digital feedwater system: *Conceptual problem:* The inactive computer tracks the actual valve demand signal from the single-loop controller. When a computer failover occurs, the control resumes using feedwater demand setpoint calculated to match the last measured valve signal output. Because this signal came from a computer in failed condition, the setpoint could be bogus, and could cause a large disturbance or trip in the feedwater system.

Single-loop controller: *Obscure behavior:* In most failure conditions, the entire display will blink or display a clear message. However, for some failures it is possible for the display to simply freeze. During normal operation, there is a single pixel in the display which is made to blink. Operators must be trained to check for the blinking pixel if in doubt about whether the system is operating.

Digitally controlled gas sampling system (shared by petrochemical): See *Example 4: Design Problem -- Gas Sample System.*

PLC replacement of solid-state devices: See *Example 2: Conceptual Problem with Transient States* and *Expample 3: Conceptual Problem -- Exhaustive Testing.*

System with remote/local units: *Conceptual problem:* A system has remote and local units with one at the point of service, and the other in the control room for display and keypad input. The control room unit is designed to reflect the mode and operation of the service unit. Rapid keypad input caused the two units to lose synchronization and function in different modes.

System with redundant processors: *Obscure behavior:* Redundant processors experienced simultaneous failures because of a software error in communications code common to both processors.

Replacement of switches: *Conceptual Problem:* An old system with six make-before-break rotary switches feeding individual solid state devices is replaced by a single rotary switch enabled by six "enable" switches feeding a PLC. Potential unforeseen behavior arises because, in the new arrangement, there are more possible input sequences which can feed the logic. Also, the speed with which rotary switches are turned may be an issue since they are scanned. If the switch passes through a position in less than one scan interval, that transient state may not be picked up.

1.3 CDR Assumptions

There are five underlying assumptions of the CDR process described in this document. These can provide guidance in considering the merits and difficulties of a CDR for a particular project, and in making adequate preparations so that the review is successful and cost-effective.

1. A CDR is not self-contained; project teams must provide appropriate follow-up
2. Almost all software has bugs, and component subsystem failures will occur
3. A digital system is comprised of a platform and an application
4. The "system" consists of the digital system, vendor processes, and the project perspective
5. Software development processes rarely function as described on paper.

A CDR is not a self-contained process; project teams must provide appropriate follow-up

The written report delivered after the review is not the end result of the CDR. The project team must resolve concerns, questions, and recommendations. For commercial equipment, the results of the CDR must be incorporated into the dedication package if they are credited in verifying the critical characteristics. Action items may be generated as a result of the CDR report. Digital hardware/software modifications, minor modifications to the engineering package, revisions to training, and/or creation of operating procedures may be indicated as mitigation strategies separate and apart from the vendor's product.

This assumption brings up another question which can help in thinking about the potential benefits of a CDR: "What is the realistic scope of actions open to the team at this point in the project?" The point of greatest potential benefit is at the completion of detailed software design, before implementation has begun.

Almost all software has bugs, and component subsystem failures will occur

This assumption is not meant to discourage the use of digital systems, but to simply acknowledge that in spite of our best efforts, equipment or subsystem failures will occur, and some of these may be due to software errors.

To initially assess potential benefits of a CDR, this assumption can be helpful. Instead of asking "How do I know this software is bug-free?" or "Can this system fail in some unusual way?" the CDR team assumes that the software has bugs and *will* fail. Instead of asking: "Can system functionality fail in such a way that no one knows the failure has occurred?" The team asserts that this will happen, and seeks to determine under what conditions this will occur.

This strategy leads to a useful question: "What high-consequence events can be caused or enabled by an unusual failure?" Pondering this question gives an idea of the potential benefit of a CDR. If a failure cannot cause serious events, then there is probably no need for a CDR. On the other hand, if a high-consequence event may be caused or enabled, then the CDR offers one way to take a closer look at the potential for bugs and failures.

A digital system is comprised of a platform and an application

There are two basic layers to any digital system: the platform layer, and the application layer. Distinguishing between these two layers is important in considering the merits of a CDR, and in preparing to conduct one.

The platform is that portion of the digital system used as a generic base for developing applications, of which the particular project under review is one. The application layer is that portion where the platform is adjusted, configured, and/or programmed to meet the requirements of the specific project.

The platform may be minimal, as in the case where the vendor has designed specialized functionality around a microprocessor, with all circuit boards and software developed in-house using development and testing tools for that processor. In this case, the platform layer consists of the microprocessor architecture together with the development tools.

On the other hand, the platform may be massive, with a complex array of hardware and/or software components which can be customized to meet the requirements of the project through a combination of the following:

- Hardware component selection and assembly,
- Software module selection and configuration (connection and option selections)
- Programming (possibly in a language unique to the platform)
- Tuning

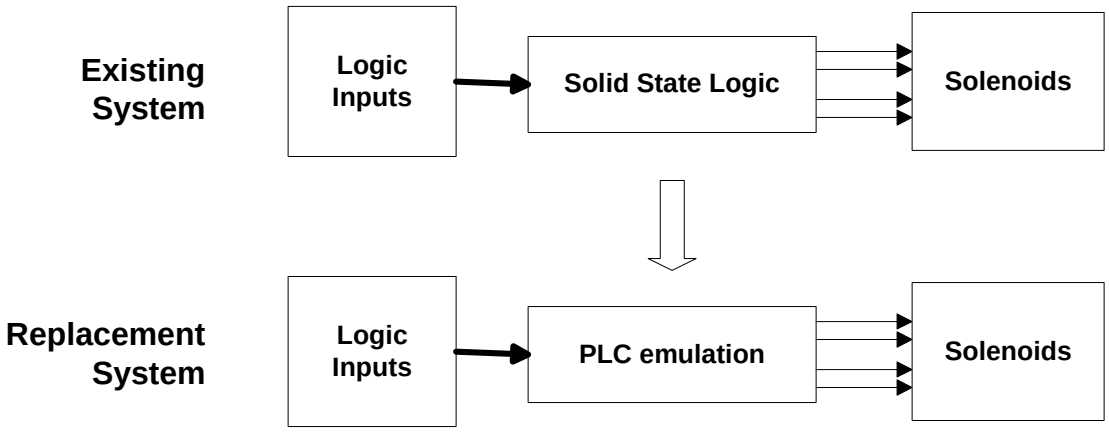
Such is often the case with Programmable Logic Controllers (PLCs) and distributed control systems.

A generic platform may have been developed by the vendor to use as a base for a family of application types, as is the case with some radiation monitoring systems. Or, it may be a commercial product (such as a PLC or distributed control system) purchased by the vendor for use in this application.

For a critical digital review to be effective, both the platform and the application must be subjected to technical questioning. A good application design residing on a poor platform will yield a poor system. A poor design residing on a good platform will also yield a poor system.

Example 1: Solid State Logic Replacement by PLC Emulation

Solid state logic is to be replaced by a system using a PLC as illustrated in the diagram below. This is to be a one-for-one replacement in which the PLC will simply replicate the existing logic. The PLC ladder logic is to be derived by mapping components and connections of the solid state device into corresponding ladder logic components.



Correct operation is to be validated by testing output values against an input-output table for all possible combinations of inputs. This is expected to provide an exhaustive test of the system's input-output behavior.

Also, it is known that with the existing system, certain "invalid" solenoid states cannot occur unless there is a malfunction. As an additional test for PLC health, a section of ladder logic will be inserted to test output values at the end of each scan cycle. On detection of an "invalid" output state, the PLC will assert a failure condition.

As discussed in subsequent examples, ***there are two conceptual problems with this plan****. First, the possibility of transient "invalid" states is not considered. In a fault-tolerant scheme with multiple PLC units, this has the potential for enabling common-cause failures****.*** Second, a system with memory cannot be exhaustively tested simply by applying known combinations of inputs.

The "real system" being scrutinized consists of the digital system, vendor processes, and project perspective

We use the term *project perspective* to mean the scope, formal requirements, and informal expectations of the project. Informal expectations are often unstated and simply assumed by project members. While these assumptions may hold for engineers familiar with the plant system in which the equipment will be applied, a vendor's engineers — who may be quite competent in their respective areas — may not understand the subtleties of a specific customer application.

A CDR must not be limited to the evaluation of the vendor's product and processes. The "real system" under scrutiny includes the informal, unstated project perspective as well.

Suppose, for example:

- There are high-consequence events that hypothetically may be enabled or caused by an unusual failure in the digital system
- There is doubt about the level of technical access to the platform to be granted to the review team
- Use of the platform is not likely to be widespread in future projects hence there will not be opportunity to gain much experience with it at the plant.

In this situation, it is unlikely that a CDR will rule out the possibility of a future event caused by an unusual failure in the system. In planning the scope of the CDR, the project team can recognize beforehand that the productive focus for mitigation is likely to be the project perspective. Perhaps the level of automation expected is higher than absolutely necessary. Maybe simple mitigation can be found in a manual bypass of the complex automation.

Project Perspective

The first task of the CDR team is to understand the project scope, formal requirements, and informal expectations. This begins before the actual CDR by reading specification documents and system descriptions, and by talking to project team members.

The CDR team must attempt to uncover underlying expectations, unstated assumptions, and any criteria that the project team will use to measure success. Here are some questions intended to help uncover this information:

Is this a Class 1E application? Clearly in these applications, there is a high degree of concern about loss of functionality due to single component failure, especially common-cause failure due to behavior of a replicated software component. In critical digital reviews the search for single-component failure modes is not confined to software, but includes the entire system.

What functions are served by this system, and how do they fit in the overall scheme of things?

What was the initial driving motivation for this upgrade?

What improvements over the old system are expected?

What are the worst conceivable consequences of (possibly silent) failure of one or more of these functions?

What human interfaces are in the control room? It is primarily through these that the operator sees and understands system behavior.

What human interfaces are outside the control room? This is a slower window to system behavior.

What process equipment does the system directly control or actuate: pumps, valves, motors?

What process variables does the system sense or measure?

What physical constraints (cables, cabinets, console space, etc.) were important in the design?

What portions of the old system are reused in the new system?

Are there informal project expectations that are assumed but not stated?

What expectations are held by the maintenance department?

Does the maintenance department have qualified technicians for this or similar equipment?

Are there expectations for self-diagnosis by the system?

Software development processes rarely function as described on paper

During the CDR, paper descriptions of software development processes and procedures will be reviewed. However, a set of verification and validation (V&V) documents that meets recommended guidance (as stated in the IEEE Standard for Software Verification and Validation Plans, IEEE Std 1012-1986, for example) can be produced independent from any actual development process. Reading impressive-looking documents may not give the utility project team a clear or accurate picture of the actual discipline, organization, and teamwork, used in developing the software of interest to the project.

During the main CDR exercise, the review team will work closely with marketing personnel, designers, programmers, and project managers. This process allows the CDR team to gain a qualitative perspective of the discipline, organization, and teamwork in the digital design, development, and support processes. This perspective is vital to determining the "value" of documentation provided.

While "retrospective" validation is better than no validation, retrospective validation does not impact the real-time development process. "Fixing" problems found in a retrospective validation may sometimes introduce more problems than it fixes.

1.4 CDR Prerequisite Information

Prerequisite input information for a Critical Digital Review has normally been generated by the end of the conceptual design stage. The CDR Team should have the following information from the project prior to the actual on-site review:

- project scope
- design objectives
- design basis
- initial risk analysis

The CDR team should consider the "unstated" or "assumed" project perspective relative to each of these areas. Many systems that meet the "documented contractual requirements" have failed in practice when they failed to meet the "intention."

Wherever possible, the CDR team should request and review any vendor literature that is available. Marketing material can often provide excellent overviews, and may illuminate the user expectations. Other customers should be contacted, and any issues noted for the review. Good preparation can minimize on-site time requirements.

The CDR team should carry any drawings, specifications, or descriptions that define the context in which the new system will be situated.

1.5 CDR Team Selection

The success of a review relies heavily on the team assembled. The team must have the technical expertise in digital systems required to penetrate the technical design of the system under review, and enough experience to exercise reasonable judgement in determining the depth of the review that is needed.

There are three functional "types" of members required for a successful CDR team:

- Lead Reviewer
- Applications Engineer
- Digital System Engineer

One person may perform more than one of these functions. Also, the titles of these individuals will vary from organization to organization, and may change depending on whether the review is done in conjunction with a formal vendor audit/survey, or as a separate design review. Note that a Certified Lead Auditor, who would normally lead an audit or survey team, may not necessarily have the technical expertise required to fulfill the role of Lead Reviewer defined here for a CDR. Another member of the team may need to serve as Technical Lead for the CDR in that case.

Lead Reviewer

The function of a Lead Reviewer is to maintain a technical overview perspective during the CDR process. In this sense, a good Lead Reviewer is a good facilitator. The Lead Reviewer must be able to:

- understand technical issues
- focus discussions
- resolve disputes
- identify root causes
- facilitate technical discussions
- provide associative skills

Ideally, the Lead Reviewer should be capable of viewing the system objectively, without undue pressure from project schedule or cost. Those with direct accountability will naturally focus on those areas for which they are most accountable.

Application Engineering

Critical Digital Reviews must be performed in the context of the application or applications for which the equipment is intended. Individuals who are knowledgeable about the application(s) are integral to the success of the review.

The individual(s) who provides the function of the Application Engineer should understand the design of the current system (including interfacing systems), the functional requirements for the new system or component, any regulatory or licensing issues, and any design basis issues. Generally, the individuals filling this role will be system engineers or design engineers.

Digital System Engineering

The individual(s) performing this function should have a good understanding of real-time software, operating systems, microprocessor design, structured analysis, and verification and validation.

These individuals should have experience with real-time process systems, understand fundamental plant systems, and understand general engineering practice (e.g., design basis, modification process).

1.6 CDR Process

Preparation for a CDR begins during the conceptual design phase of a project. The various system-related issues and risks that are defined during this stage are input for the CDR team. The CDR team itself will usually comprise a subset of the project team augmented by specialists as required.

The project team must determine the size of the CDR team, the need for specialists, the duration of the review, and the depth of the review. Parameters that should be considered include system safety/risk, system complexity, platform complexity, application complexity, customer experience, and vendor experience in the specific application.

The CDR for a well-defined project of low safety significance, and low complexity may be completed in 1 to 3 days, not including final reports. A safety significant project with relatively high complexity may require 5 days or more, not including the final report.

The critical review is usually performed at a vendor's development location. In cases where a vendor produces a product at one site, and integrates the application at another (or where one vendor uses a platform produced by another), both sites may require visits.

The actual on-site critical review follows a four-step process:

1. System Orientation
2. Process Orientation
3. Thread Analysis
4. Risk Analysis

System Orientation

The purpose of the system orientation step is to gain an overview of the vendor's system architecture. It also helps the vendor identify the members of their own staff who may be required to answer more detailed questions later in the review. The overview includes hardware architecture, software architecture, and process flow through the system.

Process Orientation

The process orientation examines the vendor's policies, procedures, and standards used in the development, documentation, testing, and maintenance of the product. Record keeping, failure investigation, and customer complaint handling are included in the review of the maintenance phase of the life cycle.

The process portion of the orientation typically does not include a critical review of the Quality Assurance organization, but may do so in cases where the CDR is integrated into a formal audit or survey.

Thread Analysis

Thread analysis follows specific functions through a vendor's documentation, testing, and implementation. Examples of thread analysis include: 1) tracing signals from field inputs through data acquisition hardware, software, and display, and 2) tracing a customer complaint from the initial call, to the failure investigation, to the design change, to the document update, and to configuration control. In the first example, the thread analysis follows a purely technical path, while in the second it follows a work process evaluating technical aspects at discrete locations. Typically, a minimum of two threads are analyzed.

The thread analysis requires penetration to the technical core by interacting with vendor design, programming, and quality staff. The CDR team strives to form a clear picture of the technical core and its relation to other aspects of the project.

This is the crucial step in the review, where the team must be prepared to work together to keep discussions on track. Team members with technical expertise must dig deep enough into internal mechanisms to get a clear understanding of potential (possibly silent) failure modes. On the other hand, team members must also guard against wasting time on technical detail that is not relevant to the issues of the project.

Risk Analysis

The final phase of the on-site CDR is the risk analysis. To optimize the coverage, both a qualitative fault tree and a qualitative failure modes analysis are performed. The qualitative fault tree will normally include predefined faults identified with input from the project team, and additional faults that the CDR team may add. The qualitative failure modes analysis postulates: failures of hardware modules, unintended software behavior, human errors, and field device failures. The failure modes are analyzed for unacceptable system behavior.

Once the on-site review is complete, the results of the CDR must be turned over to the project team for final disposition. The project team should revisit the issues on a regular basis to ensure the identified issues are resolved, and to capture any new issues which may adversely affect the project. For some projects, the CDR team may be asked to review designs as they evolve.

Conceptual Problems

Conceptual problems typically relate to the more challenging aspects of digital system design. These problems are often overlooked by application engineers unfamiliar with the subtleties of digital technology.

Finite state concepts and synchronization: Digital systems typically employ scanning (analog inputs, switches, keypads, and such are polled and sampled), serial communication (parameters sent from one unit to another using a series of discrete bits or values), shared memory, and modules where each has various modes and states. Designing the system so that all parts are consistent and in sync is a very complex task.

Component-wise emulation of solid-state devices: This is discussed in *Example 1: Solid State Replacement by PLC Emulation*, *Example 2: Conceptual Problem with Transient States*, and *Example 3: Conceptual Problem -- Exhaustive Testing*

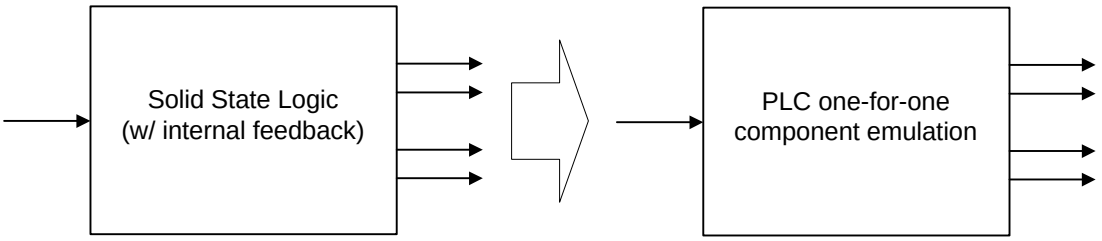
Effects of dynamics (system and process): *see Example 4: Design Problem -- Gas Sample System*

Watchdog timers: This area brings a different type of conceptual problem. It is not a technically difficult subject, but buyers often do not recognize that implementing a watchdog timer involves several important design decisions.

High speed networks: Modules on a network typically utilize common communication service routines. This creates the potential for common-cause failures. Also, high-speed networks are capable of severely loading processors unless provisions are made to protect against this.

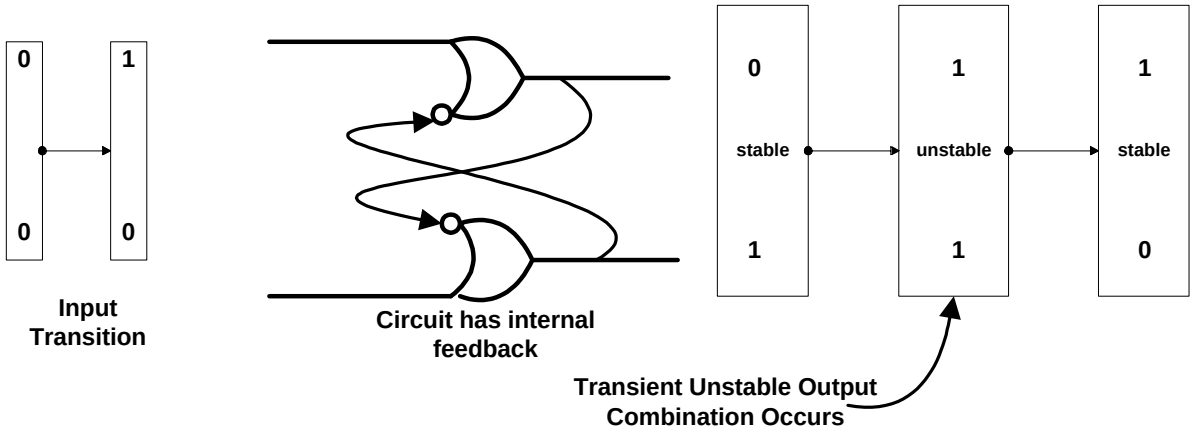
Example 2: Conceptual Problem with Transient States

A problem enters if a logic circuit contains feedback around internal components, and designers fail to consider subsequent transient behavior of the PLC emulation in response to an input transition.



In a logic circuit with feedback, certain output combinations may exist for brief periods of transition, but never appear as *stable* output values.

To see this, consider a component-level emulation of a flip-flop implemented with OR and NOT gates using feedback. This is just an illustration -- a flip-flop is an individual component within PLC programming and there is no generic issue with the utilization of flip-flops. The diagram below shows an output transition from one stable state to another forced by a nonzero input applied to the first input.



In a PLC emulation of this circuit, feedback is achieved by passing output states forward to be used as inputs to the OR gates in the subsequent scan cycle. For the input transition shown, a PLC will require two scan cycles to reach the stable output, with the transient unstable output occurring at the end of the scan cycle where the input transition is detected. Now referring back to the case of Example 1, invalid solenoid output combinations can occur at the device outputs during input state transitions. These unstable output states may exist for such a brief time that the solenoids do not respond. However, if a scheme is implemented to detect “invalid” output states, it may trigger such actions when they are not required and may be harmful in themselves.

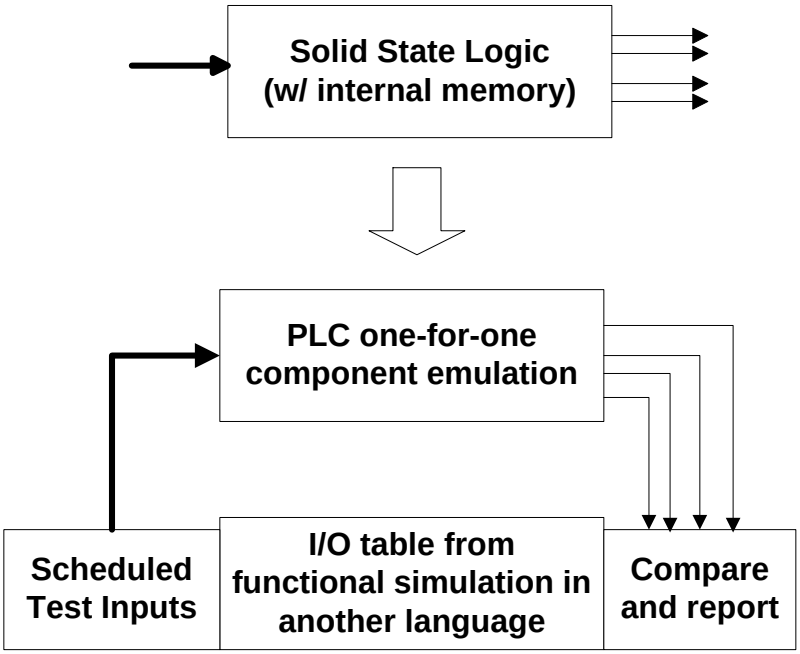
There are two general conclusions from this, suggesting the need for careful analysis in the design of PLC one-for-one component emulation replacements for solid-state circuits containing internal feedback around components:

- For some input transitions, a PLC emulation may require multiple scan cycles to converge to the stable final output value, where the number of cycles depends on internal details. If feedback is complex, correct operation may even require that input values be latched until transients are done.

- It may not be correct to treat the occurrence of an unstable output combination as an error. In fact, this itself can cause more severe failures to occur.

Example 3: Conceptual Problem-Exhaustive Testing

In formulating test plans for a PLC emulation of a solid-state circuit with internal flip-flops (or other forms of memory), a conceptual problem can occur with respect to the assumption of exhaustive testing.



In a logic circuit which utilizes flip-flops (or other memory devices), the relationship between the output values and the input values is not static; that is, the output values depend not only on the current input values, but on previous input values as well.

A test sequence which simply cycles through all possible input combinations will not achieve exhaustive testing if the logic circuit has memory. An exhaustive sequence basically requires that every reachable set of internal flip-flop values must be combined with every possible set of input values. A test procedure would call for the application of a set of sequences, where each sequence can be thought of as having two parts: the first part of the sequence drives the internal flip-flops to one achievable combination, and the second part applies one of the possible input combinations.

For all but very simple logic devices, it is extremely challenging to design a feasible test procedure which can be shown to achieve exhaustive testing.

2 Critical Digital Review

2.1 System Orientation

2.1.1 Purpose

The purposes of the system orientation are:

1. Introduce the CDR Team and its function to the vendor
2. Gain an overview of the system architecture
3. Identify topics for focused technical discussion
4. Identify and schedule vendor resources for remaining steps.

The system orientation will set the expectations for the remainder of the review. Many vendors are accustomed to audits where the customer focuses on the Quality Assurance process, often to the exclusion of the product itself. It is good to stress before the visit that the team will need access to design and programming expertise knowledgeable of the specific product.

2.1.2 Method

Vendors should be alerted to the technical nature of the CDR when first setting up the meetings. They should be informed that they will be asked to provide system overviews, describe their hardware architecture, and describe their software architecture.

They should also be informed that parts of the review will look at procedures, and other parts will entail technical question and answer sessions. The vendor should not, however, be given a detailed agenda for which they must prepare. The CDR team must have the flexibility to follow emergent paths and concerns without being constrained by rigid schedules.

Most importantly, the vendor should understand the technical nature of the review, and should be asked to have their technical design staff available to answer detailed questions.

Introductions

The CDR should start with an introduction of team members. The team members should describe their area of expertise, and their experience. This introduction provides

the vendor with a point of reference. The Lead Reviewer should provide an overview of the CDR, and the objective of the review.

The vendor should then be asked to introduce their team in a similar fashion. CDR team members should note the members of the vendor team who represent their area of interest.

System Overview

The vendor is asked to provide a system overview, showing the basic components and the functional flow of information and control. This overview allows the vendor to utilize presentation material they may already have, and allows the review to start in a non-threatening atmosphere.

The CDR team should note areas of interest during the overview, but leave detailed questioning for the architecture descriptions.

Hardware Architecture

Describing the hardware architecture will usually entail the use of system drawings. The CDR team should utilize this discussion to familiarize themselves with the various drawings that are available.

If formal drawings are not offered, the CDR team should request them. While not every drawing may be reviewed at this time, the availability, the quality, and the formality of drawings should be noted.

This is also an opportunity to begin the technical penetration of the vendor design. The CDR team should critically examine the architecture, and begin to consider possible failure scenarios. The team should avoid detailed discussions of specific failure scenarios at this point, but should note issues that may need to be pursued during the failure investigation.

Figure A-2 provides a list of suggested questions. These questions should *not be used as a checklist*, but should facilitate discussions.

Detailed questioning at this point will also ensure that the vendor has assembled the proper level of technical staff to answer these questions. When questions cannot be answered by the personnel available, the vendor should be requested to take the question as an action item, and a list of action items should be maintained.

Figure A-2. Hardware Architecture Questions

Platform/Application
PLC platform? Distributed control platform? Other module-configuration platform? Some vendors create their own platform to use as a base for a variety of applications. Some suppliers of radiation monitoring systems, for example, take this approach.

Hardware Complexity
System complexity directly impacts the level of review effort. What make/model is the main processor? They range from simple to very complex. Does the design use redundant components for fault tolerance?

Is functionality distributed over remote/local units? Are instructions executed by the main CPU distributed over multiple boards? Do multiple processors share memory?

Do boards other than the main CPU board have processors? If so, what make/models are used? If there are multiple CPU's, how do they communicate? Network? Serial? Shared Memory?

Does the hardware use an ASIC (Application Specific Integrated Circuit)? If so, what are the functions?

Which boards and circuits are required, and which are optional? Which boards are to be used in this project?

Watchdog Timers
Is there a watchdog timer? If so, is the watchdog timer a separate device or part of the CPU? What circuits respond to the watchdog timeout signal? Does timeout cause the equivalent of a power-up reset?

External Interfaces
What are the visible components and/or indications in the control room? What points of surveillance? What transducers does the hardware manipulate for control? What sensors are used to generate analog/digital inputs? What signals are generated as system outputs? Are there external clocks?

Processor/Auxiliary Board(s)
Is the memory error correcting? Do other boards have processors? How do they communicate? Is there a separate I/O processor? Does it control trouble/alert/alarm contacts? Does the design use redundant components for fault tolerance?

What is the modular organization of the boards and circuits? What external switches and contacts generate inputs to the software? Is the hardware designed for program loading as a manufacturing step? Is the system designed to save parameters and data on power dips and/or power failure? Which boards and circuits are required, and which are optional?

Analog to Digital (A/D) and Digital to Analog (D/A) Converters
Are there individual A/D and or D/A converters or does one serve multiple channels? How many channels are there? If one converter serves multiple channels, how many does it serve? Are sample and hold circuits used? Does the hardware support A/D or D/A functional or calibration checks?

EMI/RFI
Has the design minimized potential EMI/RFI concerns? Has the system been tested against EMI/RFI standards? If a digital system is not adequately protected against interference of this type, bits can get flipped and cause unforeseen behavior. (Standards are clear and testing expertise exists, so the CDR generally just touches this area lightly.)

Software Architecture

Describing software architecture is generally more problematic for vendors than describing hardware architecture. The software architecture is typically not available as drawings in documentation. The digital specialist on the CDR team should ask the developers to sketch the major software components on a white board if no documentation exists, or if the documentation is not sufficient for a critical examination.

An impromptu sketch will often reveal more about the software architecture than a ten page write up. Any sketches or white board drawings should be captured by the CDR team. Where possible, the software architecture should be left on the board for reference during the remainder of the review.

Figure A-3 provides a list of suggested questions. These questions should *not be used as a checklist,* but should facilitate discussions.

2.1.3 Results

Having established a base understanding of the system, the CDR team is now in a better position to determine which areas are most critical. If the hardware is essentially commercial equipment bought as commodity items, there will be different concerns than if the equipment is custom designed and manufactured. Likewise, if the software is running on a solid, well-known platform, the concerns will be different than if the coding is completely custom.

Figure A-3. Software Architecture Questions

Platform/Application
Commercial real-time operating system? Embedded real-time kernel/executive? Is program development in Assembly, C, C++, Basic, or Fortran required as part of this project?
Are custom "blocks" or "modules" required as part of the development in this project? It is common for distributed computer control vendors to offer programmable modules which can be programmed in a simple language similar to Basic. These can be programmed and then "connected" to conventional blocks.

Software Lineage
What does the family tree look like for this architecture, and where does this variation fit? Can the vendor give a clear depiction of the architecture, separate from the details? Can a clear picture be presented on the utilization of global variables? Can core software for the base architecture be "configured" for a wide variety of situations?

Language, Compilers, Tools
What language, or languages, is the source code written in? What tools were used? Are tools and compilers supported by the vendor (e.g., is the latest version being used)?

Task Structures
How is the software partitioned? How does data flow through the system?
Is there any critical timing? If so, how is the timing ensured? What happens if the timing is off?
Do portions of the software behave as a state machine? Are there state diagrams?
Are distributed state-machine portions required to stay in sync? What methods are used?
Are there continuous control loops executed by the software?
To what extent were object oriented and/or structured programming methods used?
What real-time engineering calculations are required in the application?
Are value changes in global variables localized in a clear manner?
Are there re-entrant tasks? If so, what considerations have been given to stack overflow?

Operating System
Does the system make use of an operating system? If so, which one?
Does the operating system use stacks (if the answer is no, then the chances are they don't understand the operating system)? If so, what analysis or provisions have been made to ensure that stack overflow does not occur?
Is the system multi-tasking? Does the system use time-slicing? Priority scheduling?

Watchdog Timers
Does the system make use of watchdog timers? If so, are they implemented in hardware or software? If software, what happens if a processor quits? If hardware, where is the timer reset in the software? Is the watchdog reset in more than one location?

Use of Interrupts
Are interrupts used in the system? Are the interrupts maskable? If so, are they ever masked?

Communication Protocols
Does the system use or communicate with distributed processors? Is the communication protocol token passing? If so, what happens when a token is dropped? Are distributed devices polled? If so, what happens if they do not respond? Is the protocol Ethernet? If so, what is the limitation on the number of distributed devices? Are broadcast messages allowed? If so, what would happen during a broadcast storm (i.e., a processor gets stuck in a loop sending out broadcast messages)? Are devices interrupted to service communication requests from other processors?

2.2 Process Orientation

2.2.1 Purpose

The purpose of the process orientation is to review the vendor's Quality Assurance program, processes, standards, and procedures. This is not a formal audit, but could be combined with one.

The basic goals of this review are to determine how a vendor expects to:

- develop products
- support products
- maintain products

A vendor's processes and procedures are likely to change through time. The procedures reviewed during a CDR may not reflect the process and procedures that were used during the product development. However, a vendor's current practice may reveal maturity, innovation, or lack of understanding.

The review will provide the CDR team with a context in which to view the product. Based on this context, the CDR team can focus their attention to spend less time in areas where a vendor shows strength, and more time in areas of greater concern.

NOTE:

A complete lack of standards and/or procedures, even for a commercial vendor, is a clear warning sign. A utility should proceed with such vendors only if: 1) there is a clear need that only this vendor can meet, 2) the utility is willing to perform and document in-depth design reviews, code reviews, and test procedures, and 3) the utility is willing to maintain the complete design basis of the product.

2.2.2 Method

The CDR team should request copies of any applicable procedures and/or standards prior to on-site visits. Reviewing procedures prior to a visit can save all parties valuable time.

While reviewing procedures, the CDR team should look for indications that may provide insight into the process. Items to note include:

- approval dates
- revision numbers
- authors
- reviewers/approvers

Approval dates should be compared against the product development dates. Procedures that were approved after a product was developed may simply indicate the codification of prior informal practices, or may indicate a lack of prior control.

Revision numbers may indicate that a process has been refined through time, or indicate recent attempts to meet ISO standards.

The authors of various procedures may indicate how the organization works. Do the technical experts write the procedures they will live by, or does a QA organization dictate rules and regulations?

The reviewer and approval signatures, or lack of signatures, on a document can also reveal the level at which procedures are reviewed. Do the reviewers report to the author organizationally? Do the reviewers/approvers have an equivalent, or better, level of expertise as the author? Do the author, reviewers, and approver work for the same organization?

While no single item can be used to gauge an entire system, the total aggregate of items may. Again, this orientation is not an audit. While this process may provide a good starting point for a formal audit of procedures and practices, the CDR team's focus is the digital device.

Figure A-4 provides a list of suggested areas for review. This should *not be used as a checklist,* but should facilitate discussions.

2.2.3 Results

The process orientation provides a point of reference for the CDR team. If a company is found to have no procedures, or inadequate procedures, the ability to utilize the product will rest solely upon the technical basis. The utility that buys a product from a vendor such as this must be prepared to compensate for the process deficiencies. This may entail the purchase of source code and development tools, or providing assistance to the vendor to establish proper controls.

Figure A-4. Process Orientation Questions

Organization
Organizational charts show reporting chains. If a separate Quality Assurance organization exists, do they report to higher levels of management where they are not unduly influenced by the pressures of project schedules and budget?

The organizational charts should also be reviewed to determine the size and depth of the technical organization. Does the organization rely on single individuals for key functions (e.g., programming)? If so, can the organization perform qualified peer reviews?

Document Control and Distribution
If the organization has formal standards and procedures, how are they controlled? How does the technical staff access the documents? How is the staff notified when procedures are modified or created? Who is responsible for ensuring that all manuals are maintained up-to-date?

Development Process
Does the organization have a defined development process? Are deliverables from each project phase clearly defined? Are requirements reviewed and approved? Is there a formal independent verification and validation program? Are design review meetings held? Are there code walk-throughs? How are comments and action items captured and tracked? Is there a formal risk assessment? Is there a testing methodology that ensures both documented module and system level testing? Does the testing methodology require that all boundary conditions be tested?

Configuration Control
How does the organization control software and firmware revisions? How are design documents controlled? Can the source code for embedded PROMs (where applicable) be found? Are development tools such as compilers archived with product software? Are all versions of released software and firmware maintained? How are revisions identified for firmware? Can modifications to hardware or software be made without issuing new customer discernible model or revision labels?

Customer Service and Complaints
Does the vendor have a customer service policy? Are knowledgeable staff available during off hours? Are all calls documented and tracked? Is there a clear process for identifying system errors? How are customer returns handled? Are hardware boards upgraded automatically? Can customers request specific revision levels be maintained when having repairs made, or when ordering spare parts?

Error Tracking and Reporting
Is there a clear procedure for handling error reports? Is there a customer notification process? If so, who is contacted and how? Are open error reports available for customer review? How is an error report tracked and closed?

Failure Investigation
Do error reports result in failure investigations? Are failure reports reviewed with management? Are bugs merely fixed, or do failure investigations look for root causes? Are prior products, or revisions to existing products checked for similar problems? Are failures/errors tracked and trended for "big picture" analysis?

The process orientation also provides the CDR team with an overview of the development, complaint handling, failure reporting, and modification mechanisms. The use of and adherence to these mechanisms will be verified during the thread audits that follow.

The CDR team should note any issues that have surfaced during this review. Examples of issues that may arise are 1) the customer needs to subscribe to an upgrade service to be notified of the latest field reports, or 2) hardware boards that are returned for repair have the firmware upgraded without customer notification unless otherwise requested.

2.3 Thread Analysis

2.3.1 Purpose

The "thread analysis" serves three functions. First, the analysis helps to verify the information and processes that have already been discussed. Second, the analysis helps to reveal "informal" practices and "tribal knowledge." Lastly, the thread analysis provides a detailed, in-depth sample of the product's integrity.

2.3.2 Method

The thread analysis is a detailed, systematic tracing of specific functions through a vendor's product and processes. The thread analysis is analogous to a statistical sampling.

Performing a detailed review of an entire product's software — which could easily exceed 100,000 lines of source code — is completely impractical. The same could be said for tracing all the requirements through design documents, drawings, and test procedures. By carefully choosing "threads to pull" we can gain a reasonable level of confidence, or concern, in the product.

Selecting Threads

Selecting threads to pull is the first step in the Thread Analysis. While certain critical threads (e.g., safety shutdown) can be determined prior to the CDR based on the application, the CDR team should utilize the experience they have gained up to this point in the review to select other threads to pull.

Individual team members may, at this point, have found specific items of concern, or interest. If the vendor has adequate resources — and a lack of resources may or may not be of concern — each team member may choose to pull his or her own thread. The CDR team should, however, understand what each thread will be, and who has adequate technical knowledge to follow the thread.

For small systems, where the criticality of the system is relatively low, two threads may be adequate. Most systems, however, should be subject to no less than three threads, and possibly more depending on the criticality and complexity of the device or platform.

The chosen threads should, at a minimum, contain one process and one technical thread (see Figure A-5).

Where a system is distributed, the CDR team may want to consider pulling threads for each distributed unit, and one or two that will follow the integrated platform.

Items For Consideration

The basic areas that should be considered during the thread analysis include:

- physical product
- software
- documentation
- vendor processes

The physical product includes all of the various hardware components that comprise the device, plus any auxiliary components (e.g., handheld programming device, printers, display devices).

The software includes the software residing in the device, plus any software used to build, maintain, or otherwise develop the system (e.g., compilers, assemblers, operating systems, automated test programs).

The documentation includes requirements documents, design documents, drawings, manuals, test procedures, error reports, failure analysis documentation, customer complaint records, and any other documentation that was either created with the product, supports the product's use, or documents the product's behavior.

The vendor processes include all processes reviewed during the process orientation, plus any processes that are internal to the development, support, or maintenance functions that are revealed during the analysis.

Figure A-5. Thread Analysis

Process Thread
To perform a process thread, find a system error or failure that led to a revision of either hardware or software. If possible, find a fault that was initially reported by a customer.

First, trace the reporting mechanism. Ask to see the initial call report, or complaint/error form. Does the vendor form provide critical data such as date reported, party reporting event, product affected, description of the problem, and some unique identifier?

From the initial report, trace the complaint to the modification process. Is there any indication of root cause analysis, or are "bugs" merely "fixed?" Are errors communicated to existing customers? Are previous releases or products which share similar design features reviewed for common problems?

Are all of the requirements and design documents reviewed and revised to ensure any changes are adequately reflected? Are changes to software documented in the source listings?

Is regression testing performed? Who determines what testing is adequate? Are changes tested with older versions to ensure compatibility where both old and new designs may co-exist?

How are changes communicated to the production process? How is the final change package approved, and by whom?

Technical Thread
A technical thread will follow a product function from input to output. A typical thread would start with a signal from the field device. The thread, in this case, is application independent (unless, of course, the device performs only a specialized function). The purpose of this thread is to evaluate the core functions of the product, or platform.

First, the bounds of the device are defined for both normal and failed conditions. Failed conditions may include high, low, cycling, or shorted.

The signal is then traced into the data acquisition hardware. Questions to ask include what type of analog-to-digital converter (ADC) is being used, and is the ADC dedicated to a single input, card, or system? How frequently is the signal converted? Where is the value stored? Is the signal filtered? If so, how? Is there any protection from field surges?

Check design documents for accuracy and completeness.

How does the output signal get generated? Does the system verify output signals to the field? If so, how?

Check test documents for completeness. Was this signal path covered in the testing? Under what conditions?

Application Thread
Choose a critical function from the application for which this system is being considered. For example, shutdown of some pump. From here, the thread is pulled in the same fashion as a technical thread.

How to Pull the Thread

As the Mad Hatter said in Alice In Wonderland, start at the beginning, and when you get to the end, stop.

The starting point for pulling a thread begins at one end of the thread. One example of a thread end might be the conceptual or requirements document. The other end of the thread may be the actual source code for a module, or an A/D converter. The beginning and end points will differ depending on the vendor, the findings up to this point in the review, and the areas of most concern.

The CDR team should determine their starting points without regard for what the vendor has or has not defined in their process overview. While this may seem counter-intuitive (e.g., why start with the requirements document if they have said they don't have one), the point in the thread review is to re-construct the development process and discover what actually exists.

What to Look for

Vendors may have good procedures that aren't followed, excellent procedures that are followed, or even informal, non-codified processes that exhibit technical excellence.

Similarly, vendors with good procedures that are followed do not necessarily produce high quality, technically sound products.

Emphasis should be placed on technical merit, not dotted "i's" or crossed "t's." However, meticulous documentation may provide an indication of technical excellence; sloppy documentation may reflect questionable practice.

If starting, say, from the requirements end of a thread for alarm checking, the first question to pose is simply: "Can you show us where the requirements for alarm checking are first stated?"

Commercial vendors may not subscribe to waterfall development methodologies, and may not have a neatly defined "System Requirements Document." However, the vendor should be capable of producing some artifact that describes the alarm checking requirements.

If a vendor produces a user reference manual, which is usually produced after development, the CDR team should continue to pursue the questioning. The developers can be asked how they knew to write software for an alarm checking function. Often, this line of questioning will reveal the internal development practices.

From requirements, the questioning should lead to design documents, test documents, code and detailed hardware layouts. At each stage, the reviewers should look for both formal and informal practices.

At the software module level, the reviewer should note items such as headers, comments within the code, readability of the code, use of global commons or data hiding techniques. If code has been written by numerous individuals, the CDR team should ensure that they examine several portions of code to determine if there is consistency in the coding practices. If there are written coding standards, the code should be compared against the standard.

Hardware design should go through a similar design review. Separation of tracing on boards, the use of jumpers, polarized capacitors (which may work in the reversed direction for short testing periods), hand versus machine stuffed boards, and ESD handling should all be considered.

Process Threads will follow a similar route, but the threads will extend into customer notification procedures, error reporting, change control, configuration control, and regression testing. The same documents that are reviewed for the technical threads should also be reviewed to determine if they have been updated. Software coding and/or hardware drawings should be examined to determine if changes have been clearly identified.

At each stage reviewers should look for evidence of technical reviews, noting their independence, formality (e.g., are there action items?), and follow-through. Lack of technical reviews should raise concerns.

2.3.3 Results

Thread Analysis can answer the following questions:

- Are vendor procedures followed by the staff?
- Is documentation planned, or an afterthought?
- Are technical reviews performed on a regular basis?
- Is there a well maintained design basis?
- Are changes to the design adequately managed?
- Are customers notified of errors?
- Is the software well structured and understood?

- Is the staff knowledgeable?
- Do informal practices need to be documented?

While negative answers to some of these questions may not eliminate the need or desire to use a specific product, they may lead to new requirements for the vendor and/or project team. If a vendor shows poor configuration control, the utility may need to negotiate the rights to design documentation. If a vendor has not performed technical reviews, a project team may want the CDR team to increase the scope of the review, and may require more extensive testing.

The analysis can also deepen the CDR team's knowledge of the internal mechanisms of the product. This knowledge is critical in the final phase of the CDR, the risk analysis.

Watchdog Timers

***Is there a watchdog timer*?** The answer is usually yes. Without a watchdog component, time-critical tasks may degrade or cease to function entirely with no positive indication that this has happened.

Is the watchdog timer a separate device or part of the CPU? Many computer chips have a built-in watchdog timer circuit, which gives only limited protection against processor "hangup" short of a chip failure. If the chip itself fails completely, then functionality of both the CPU and the watchdog timer may be lost.

Does timeout cause the equivalent of a power-up reset? In many cases, the design philosophy of the watchdog timer is that it should force an "automatic reboot" to restart the system if it hangs up for any reason. Under this design philosophy a watchdog timeout may have exactly the same effect as rebooting the system. This may or may not be acceptable for the planned application.

Does the watchdog timeout event cause a latched indicator or contact closure? If the event causes a power-up reset, there may be an external indicator or contact closure that is latched to show that a reset has occurred.

What circuits respond to the watchdog timeout signal? In more sophisticated systems, the watchdog timeout signal may be used to directly control the behavior of subsystems. It may, for example, cause output signals to go to a pre-determined state independent of the CPU. Circuits may be designed to force operator displays into a blinking mode on watchdog timeout.

Topic for Focused Discussion: Watchdog Task Coverage

A *watchdog timer* protects against failure of the CPU to perform a task, or a set of tasks within a specified amount of time. It has a clocked counter which counts down from an initial value at a fixed rate, and it has a digital input by which the CPU can send a pulse to reset the counter to its initial value. In the event that the timer counts down to zero before the reset pulse occurs, a *time-out signal or event* is generated.

The mere presence of a watchdog circuit does not mean that all critical tasks are protected against time-performance degradation. The "task coverage" of watchdog protection is determined by the organization of tasks and the manner in which timer reset functionality is implemented within those tasks. In design reviews, it is not rare to find that the watchdog timer fails to protect critical tasks against time -degradation. In some cases, one finds that the watchdog protects only against complete failure of the CPU.

To determine "task coverage" of the watchdog timer the review team must understand the specific task organization of the application, the use of interrupts, and the details of where watchdog reset occurs within the software. Typical task organization and the relevant watchdog issues are discussed below.

One common task organization: Background/Foreground
In simple real-time applications, software is often separated into just two sections, one of which is a small streamlined task triggered by a clock-driven interrupt so that it executes at regular time intervals, providing the "heartbeat" of the application. At every tick of the clock, this *foreground* portion performs input-output housekeeping, and increments a counter used by the other software section for timing.

At each clock tick, foreground interrupts the other section, *background* , which executes from some starting point to an end point where it branches back to the beginning. Sometimes the frequency of background execution is limited with an idle loop at the end which continually checks the contents of a service counter (incremented by the foreground portion). When the counter equals or exceeds a specified value, the background section exits the idle loop, resets the counter, and branches back to the start.

A watchdog may protect against only foreground degradation, against only background degradation, or against degradation in either section. If the watchdog is reset unconditionally in the foreground section, then there is no protection against background degradation. Even if background enters a tight infinite loop, foreground executes every clock tick and resets the watchdog.

One common way to protect both foreground and background is to put the reset portion in foreground, but with logic requiring the setting of an "I'm alive" flag by background since the previous watchdog reset.

Another common organization: Executive with scheduled, prioritized tasks
In more complex real-time applications, software is organized into concurrent tasks which are marked for execution using service counters, and receive execution time based on assigned priority. There is still a "heartbeat" section (called the *executive* or *kernel*) driven by a clock interrupt, whose main job is to maintain timing counters for each task, to mark tasks for execution, and to pass execution to the highest priority task marked for execution.

In software organized in this way, it is possible for tasks to be "locked out" by higher priority tasks, and if reset, functionality is placed in higher priority tasks, no watchdog timeout will signal the event.

2.4 Qualitative Risk Analysis

The Qualitative Risk Analysis can be the most important facet of the CDR. This activity will use the knowledge gained in the previous sections to help answer the questions: "Is the use of this digital product a reasonable solution? Are there risks of undesirable behavior?"

This phase combines both a qualitative FTA and a qualitative FMEA approach. The term "qualitative" is used deliberately to avoid any confusion with formal FTA or FMEA approaches that seek to quantify failure potential and reliability. No method for predicting software failures or software design errors has been established for the diverse range of digital devices that utilities are likely to use.

Experience has shown that no single method of risk analysis can provide full coverage of all risks. Studies have shown, however, that combining a top-down method with a bottom-up method provides better coverage than either method alone. While the use of a combined method increases coverage, no method or combination of methods can guarantee full coverage of all potential risks.

Figure A-6 provides a list of suggested areas for investigation. These should *not be used as a checklist*, but should facilitate discussions.

2.4.1 Prerequisites

The Risk Analysis requires in-depth knowledge of software, hardware, interfaces, operation, and application. The vendor should be asked to have knowledgeable staff present during these sessions.

The CDR team, having examined the various system documents, should specify which documents need to be available during the sessions. These documents may include both formal and informal documents.

System Architecture documents, which are critical for the review, are most useful in the form of drawings and/or diagrams.

The ideal set of documentation for software architecture would include information regarding the following:

- software partitioning
- flow of data
- flow of control

- critical timing and throughput
- hardware interfaces

Hardware architecture documentation should include information and drawings for the actual boards in the computer/microprocessor device, and defined interfaces to/from all controlled devices.

Buyer/Supplier Confusion: Vibration Monitor

A vibration monitor used in an automatic vibration trip system was to be upgraded to a new digital version. A CDR of the trip system turned up no significant problems with the supplier's design, but it did reveal buyer/supplier confusion.

The supplier's line of equipment contains functionality for automatic trip protection, and for maintenance management. The basic trip-protection subsystem uses an array of real-time signal-processing modules to test properties of probe signals against limits. It also sends detailed sampled values to a separate PC with data analysis and maintenance management packages.

Some mechanical problems (such as bearing pre-load condition) do not give high vibration symptoms directly; rather, they give symptoms which show up in the phase relationship between signals from physically orthogonal bearing probes. The supplier offers two types of functionality to detect changes in phase relationships: 1) there is a trip-protection module which monitors phase and trips on significant change, and 2) there are maintenance management software modules which will reveal such problems through trends applied to historical data.

The system was specified and ordered by the I&C department. The order included standard trip-protection modules (but no phase trips), and the maintenance-management option with a separate PC and data analysis software, but this was done with no input or commitment by the maintenance department to include data analysis in the work process.

The supplier assumed that the customer had sorted through the alternatives of automatic trip-protection vs. off-line trend analysis and had made an informed decision that no trip protection modules were needed for phase relationships.

2.4.2 Qualitative Fault Tree Analysis

The fault tree analysis works from undesired states or hazards, and then works back to determine the potential cause(s) of the undesired states. The FTA is documented in a fault tree diagram where the primary event is at the top of each tree. Events and/or conditions that must be present to cause this primary event are drawn under the primary event with lines connecting the two. Where needed, "and" gates should be

shown; "or" gates are implicit. Each new event is then de-constructed in a similar fashion until basic events have been uncovered.

What constitutes a "basic" event is an arbitrary decision. The basic events should provide the CDR and Project teams with enough information on which to base design decisions. For example, "software failure" would not provide adequate information, while "infinite loop in calculation module" could. For the second example, the code in the calculation module could be walked through in detail to determine if there were any iterative loops that could diverge.

Hazard Identification

Defining the undesired or hazardous states is the first step in the FTA. The question the CDR team should be asking is: "What are the worst things this device could do?"

The project team should have identified many of the system level hazards prior to the CDR, but the CDR team should use their recent knowledge of the system to postulate additional hazards.

For most systems, there will be numerous "worst things." System failure, while an obvious "worst thing," is only a beginning. What if a device fails without indication? What if the system ceases to properly calculate values? What if the system fails in such a way as to give the appearance of working (e.g., lights remain lit and there is no visible indication of failure)?

Fault Tree Construction

For each "worst thing," construct a tree starting at the top with the undesired state, and show what states or events would have to occur to cause this event.

Each subsequent event or state is decomposed until initial events are found which cannot be decomposed. (As noted earlier, this is often an arbitrary decision.)

2.4.3 Qualitative Failure Modes and Effects Analysis

The qualitative FMEA postulates failures at a module level — both hardware and software — and determines the effects at both local and system levels. For each postulated module failure, the CDR team should determine and document:

- the postulated failure
- the effects of the postulated failure

- possible causes of the failure
- possible mitigating actions/design features

For each module, there may be several potential failures to consider.

Assemble Drawings and Specifications

The use of system architecture drawings for the digital, electrical, and mechanical sub-systems is required to perform the analysis. Software architecture drawings or sketches from the system orientation should be available.

Postulate Failures of Modules

Using the drawings, identify modules. A module can be a complete computer, a board in a computer, or a component on a computer board. Module sizing should be chosen according to the perceived system threats.

If a computer is being used merely to record data, then the computer may be viewed as a "module" during the initial pass. However, if a computer board is being relied upon for an emergency shutdown, then the board itself would be a more appropriate module choice.

Software modules should also be chosen in the same fashion. For some applications, a task composed of numerous subroutines may be the appropriate module size, but for others, the subroutine itself may be the appropriate size.

Each module is assumed to fail. For the initial pass, do not consider the likelihood of failure. (A high consequence, low probability failure led to the Bhopal disaster.)

Software, which is really a set of "instructions," cannot by definition "fail," but it may introduce "faults." Many software attributed failures are often the result of compromised or faulty memory locations. Bad indexing, altered program counters (bit flipping), and a host of other hardware-related failures can cause tasks to abort. While these failures may initiate in hardware, the effect on the software is what we must define.

The modules chosen are somewhat arbitrary in terms of defining what makes up a module. In general, when a chosen module can be the cause of a serious failure, the decomposition of the module into smaller modules may be warranted. For example, if the undetected failure of an I/O module can cause human harm, then the I/O module may require further decomposition to understand the failure modes internal to the module in order to determine the likelihood of the failure occurring.

Identify Failure(s)

For each module, identify the failure. For some modules, there may be multiple failure modes. For instance, a software module may simply abort, or the module may become trapped in an infinite loop. A pump may also fail in several ways, each having a different effect.

Determine the Effects of Failure

Once the modules are chosen and the failure modes defined, the effect of each module failure is traced through the system. The effect of this failure is then documented.

Careful attention should be paid to the human factor in each failure. If the operator of the device has clear and unambiguous indication of the failure, the effect may be minimal compared with that of a silent, undetected failure.

Identify Probable Causes

For each failure, identify potential causes of the failure. For instance, processor reboots or random memory failures may be the result of a power surge.

Identify Mitigating Actions and/or Design Decisions/Changes

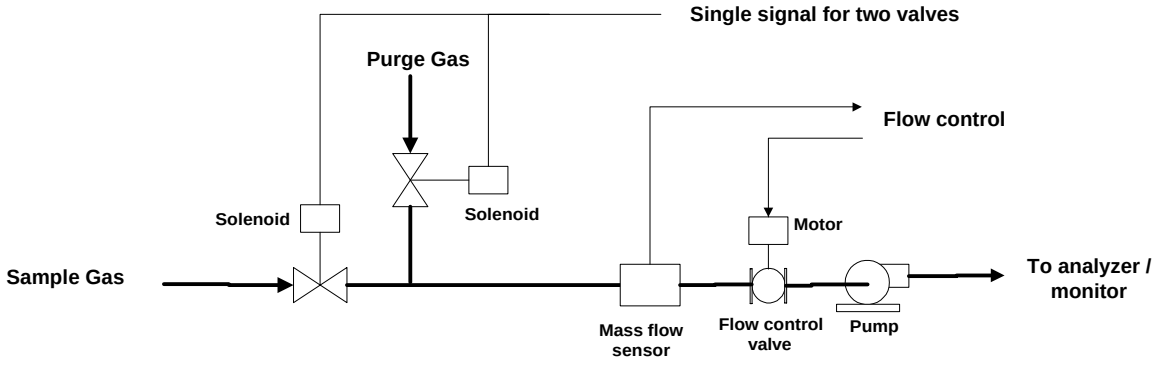
For each failure, determine what actions could be taken to either prevent or mitigate the consequence of the failure.

Example 4: Design Problem-Gas Sample System

One driving force for technical questioning during a CDR is the question of whether the team can identify credible silent failure scenarios, where system functionality may be lost with no subsequent indication in the control room or at points of routine surveillance.

To explore this question, the technical team must gain an understanding of the non-digital components of the application, and the interaction of those parts with the digital portion.

The diagram below shows the skeleton of a digitally controlled sampling system which might be found in a nuclear or petrochemical application. It will be used to illustrate two failure modes.



Failure of the purge valve to the open position

Consider this credible silent failure scenario: Should the purge valve stick in the open position, an unknown mixture of purge air and sample gas will flow from the sampling system. There will be no indication in the control room or at the sampling skid. If purge gas is similar to "normal" sample gas, then all systems will appear to be functioning normally with the purge gas valve stuck open.

While this scenario does not involve a failure of the digital portion, it does expose a design problem with the digital application. An additional contact closure on the purge valve brought in as a digital input could be used to confirm closure of the purge valve.

Failure of the mass flow sensor mid-scale

The software checks sample flow against preset limits. If the mass flow exceeds these limits, then a failure is asserted. A failure of the mass flow sensor to an extreme high or extreme low value will cause such an assertion to occur.

Should the mass flow sensor "freeze" within the preset limits, however, no failure will be asserted and the flow controller will drive the valve either fully closed or fully open. If the valve goes fully closed, there will be no sample flow through the detector, and no indication that this has occurred (the flow meter gives a false indication of reasonable flow). The pump may subsequently fail with no direct indication that this has occurred.

Figure A-6. Risk Analysis Questions

System Inputs: Consider each analog input freezing mid-scale: What is the resulting behavior? Consider each analog input failing low or failing high: What is the behavior?

Software: For each section of code, suppose an infinite loop were inserted at different points: Are there software sections where inserting an infinite loop would not cause watchdog timeout?

Error Handling: How are real-time error events handled? Are CRC memory checks made at startup or during code execution? Are there any error checks which occur in real time?

System Behavior During Failure: Can the system stop functioning without my knowing it has stopped? If we do know the system has failed, can we take remedial actions in time to prevent a serious accident, a challenge to a safety system, or lost revenue? Can the system fail in such a way that false information may mislead the operators? Can a failure prevent my taking manual control? For each hardware subsystem, classify control room/surveillance behavior under different failure scenarios.

Redundancy: In redundant failover schemes, are transients and/or race conditions a factor? Can both processors become master at the same time? Can both processors become backup at the same time?

Watchdog Timer: Where is the watchdog refreshed in the code? What does the watchdog timer do when it is triggered? Does the system reboot without indication to the operator?

Multitasking: If a multitasking system is used, will failure (e.g., aborts, infinite loops) of every task be detectable?

Diagnostics: Are diagnostics run on system boot-up? Are diagnostics run in real time? What tests are run during diagnostics? Can diagnostics interfere with real-time processing?

Undocumented Software: Does the vendor leave undocumented code in the device?

3 Post Review Analysis

As stated earlier, a Critical Digital Review is assumed to be part of an overall project. The CDR team will return from the review with objective evidence that describes the vendor, the vendor's practices, the digital device(s), and the potential issues that may arise from the use of the product. The CDR team may also return with suggestions, comments, and recommendations that affect the conceptual design of the project.

The CDR team should meet after the review to discuss any overall impressions, capture any open issues left with the vendor, and determine how to present their analysis to the project team.

The CDR should be well documented. All concerns, recommendations, and identified risks should be incorporated into whatever mechanisms the project team uses to track open action items.

The project team should review the results of the CDR with the entire CDR team to ensure the correct transfer of issues and recommendations. The project team should then take ownership of the report, and ensure resolution of all items.

The *resolution* of the risks *does not mean elimination* of all risks. In some cases, the risk cannot be avoided without unwarranted expense. But mitigation of the failure by, for example, operator training, may reduce the consequences to an acceptable level.

B

SAMPLE TEST PLANS RELATED TO DIGITAL SYSTEM SIGNAL PATHS AND TIMING

This appendix provides some sample test plans for examining the performance of digital control systems, specifically in the area of signal paths and timing issues. Electricité de France (EDF) has developed and provided these test plans as part of a cooperative effort with EPRI.

EDF intends to use these to support qualification of control systems for the next generation of French nuclear power plants. For the purpose of this document, they provide examples of detailed test plans for three specific types of performance testing:

- Information transit time
- System behavior during an "avalanche"
- Time tagging

See Section 5.3 in the main body of this report for more information on testing as a method of verifying critical characteristics of digital equipment.

TABLE OF CONTENTS

1 Introduction

1.1 Context

As part of the REP 2000 project (next generation of French nuclear power plants), EDF/DER/CCC is responsible for defining the qualification process for the "Level 1" control systems. In the French multi-level I&C architecture, Level 1 includes the Plant Automation System and Safety Automation System.

In 1996, EDF/DER/CCC defined the outline of this qualification process, formalized in the document "Preliminary Qualification Programme" [PPA]. An additional document [GI] has identified the first "Investigation Groups," giving shape to the main subjects to be addressed during the qualification process. These Investigation Groups structure the process and are the entry points for the elaboration of future test and analysis programs.

In addition, EDF/DER/CCC is working with EPRI in a cooperative program on the subject of pre-qualifying commercial, off-the-shelf digital controllers and control systems to support upgrades to I&C systems in existing nuclear power plants. As part of this effort, EDF is working to define and prepare test programs on certain subjects, based on the experience gained in qualifying and operating the I&C systems in the N4 plants (the current generation of nuclear power plants being built and operated in France).

1.2 Purpose of This Document

To support these two efforts, EDF/DER/CCC is preparing test plans to serve as intermediate documents before writing down the actual test programs in detail for future systems that will be chosen by EDF for the REP 2000 project, and by EPRI for US nuclear power plants. These intermediate documents provide the test principles and outline the procedures for evaluation of Level 1 control systems. They are directly based on the experience gained with the French N4 nuclear power plants and on other work performed by the GESYC test group. They are organized around the investigation groups and themes which have been identified in the document [GI].

The present document combines three of these test planning documents, covering the following types of tests:

- Information transit times,
- System behavior during an "avalanche,"

- Time tagging.

This document is generic, i.e., it does not pre-suppose the selection of a particular system, nor even the selection of a particular overall control system architecture.

One of the objectives of these test plans is that they be sufficiently practical for direct, rapid and concrete use when preparing and performing the tests. In particular, the test plans should enable the reader who has a good knowledge of control systems to write down easily and quickly a detailed test program for each of the three test topics listed above.

Two cases or uses are intended for this document:

- A case in which the purpose is to qualify the control system for a given application. It is assumed that the reader, who will prepare the test program, will have at his disposal the following three documents:

  — the test plan presented here,

  — the control system supplier documentation, giving the system architecture and detailing its components,

  — the requirements specification document, preferably with the requirements already arranged according to the investigation groups/themes.

  This case corresponds to the qualification process within the French REP 2000 project. It also would be the case when a commercial controller or control system needs to be dedicated for a nuclear application. The test program would support the verification of critical characteristics of the control system, and validation testing of the integrated system (application and platform).

- A case in which the purpose is to assess the control system, for example, as part of a generic pre-qualification of a control system platform, without reference to a specific application. It is assumed that the reader, who will prepare the test program, needs only the following two documents:

  — the test plan presented here,

  — the control system supplier documentation, giving the system architecture and detailing its components.

  However, it is assumed here that the user will have at his disposal some typical requirements representative of nuclear power plant control systems, for example, as developed by EPRI for PLC qualification [EPRI].

2 Reference Documents

[EPRI] Generic requirements specification for qualifying a commercially available PLC for safety-related applications in Nuclear Power Plants
EPRI TR-107330, Rev. 0

[1069] Industrial process measurement and control - Evaluation of system properties for the purpose of system assessment IEC 1069

[PPA] Plan (ou Programme) Préliminaire d'Acceptation XXX A

[GI] PAS : Plan Préliminaire de qualification - Groupes d'investigation
HP-32/96/XXX A

3 Glossary

ANA: Real variable, irrespective of how it is represented (analog or numeric values), as opposed to logic variable.

Application processing: Programmed processing, adapted per variable, as opposed to systematic processing.

Assessment (of a system): Judgement, based on evidence, of the system suitability for a specific mission or class of missions [1069]. In this document, the term assessment will be used when there is no specific mission (and therefore no specific requirements), as opposed to qualification.

Event: An event, associated to an (input, output, or internal) variable, is defined as follows:

- for a **LOG variable**: an event is a change of state (0 → 1 or 1 → 0)
- for an **ANA variable**: an event is a significant variation of this variable, i.e., higher than a predefined percentage of the range of this variable.

For the purpose of this test, an event on an input shall always be considered as instantaneous, i.e., of a duration which is negligible compared to the studied characteristics.

Influencing conditions: Conditions which are external to the system, and which are likely to influence the system behavior (cf. [1069]).

Influencing parameters: These are the system parameters which are configurable for the purpose of a particular application, and which are likely to influence the properties of the system which are the subjects of the test (cf. § Modeling).

LOG: Logic variable with two possible states (0/1)

Measure: A measure is a set of repetitions, and corresponds to a given set of influencing parameters and conditions.

Path: A path represents the route taken by a signal, and is characterized by:

— its input and its output at the borders of the system;

— the physical trajectory taken by the signal (type of input card; set of processing units, communication unit, and networks used; type of output card); and

— the type of processing performed on this signal (systematic or application).

Phase: For avalanche testing, a phase is a set of sub-tests, and corresponds to a given test objective (identification of technical function limitations, behavior under contractual or typical avalanche profile, identification of maximum avalanche profile manageable by the system).

Qualification: The qualification process is the process of demonstrating whether an entity is capable of fulfilling specified requirements (ISO 8402). The qualification is the result of this process. Qualification is used in this document when a set of specified requirements does exist.

Repetition: A repetition corresponds to a given stimulation of the system under test. Each repetition is separated from the previous one by a power supply shutdown, or a re-initialization of the processing units.

Signal: Variation of a LOG or ANA variable as a function of time.

Sub-test: A sub-test is a set of measures, and corresponds to a given system configuration and a path or avalanche profile to investigate.

System under test: Representative configuration of the control system (subject of the assessment or qualification), used in the actual test.

Systematic processing: System or pre-programmed (configurable or not) processing which is potentially performed on all variables of the same kind (A/D conversion, filtering, chattering processing, etc.), as opposed to application processing.

Test: A test is a set of phases (or sub-tests if there is only one phase), and corresponds to an investigation group or theme (cf. [GI]). The themes discussed here are transit time, behavior during an avalanche, and time tagging.

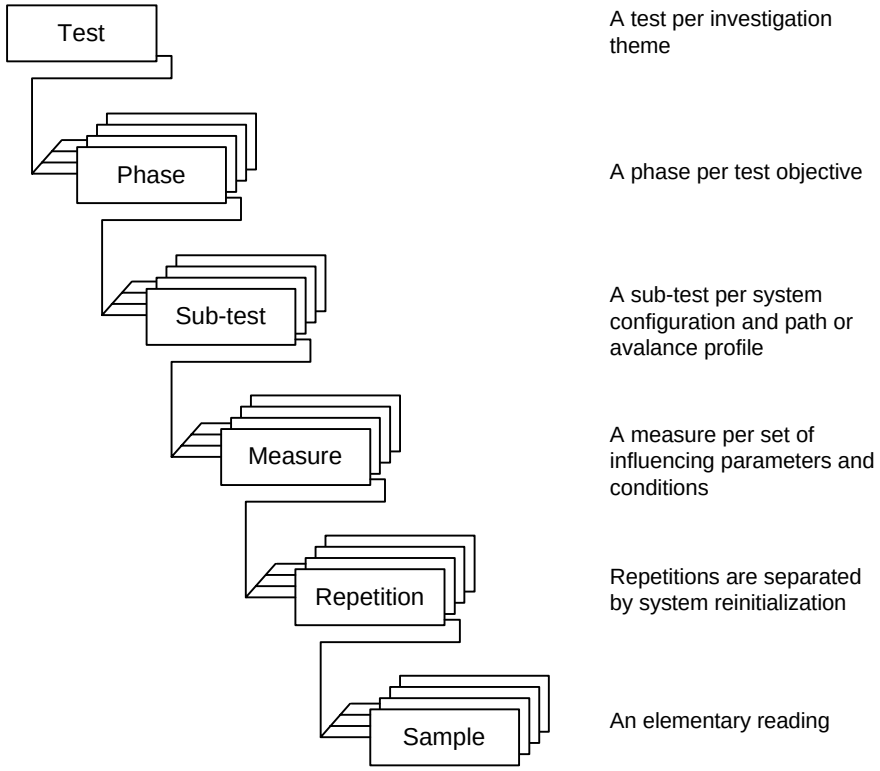


Figure B-1. Test Breakdown

Test System: Set of hardware and software, not belonging to the system under test, and necessary to perform the tests, enabling in particular the system (under test) input stimulation and output monitoring.

Transit Time: The duration of time between occurrence of a defined event at the input to the control system and a corresponding event at the output. A more detailed definition is given in Section 5.3.2.1.

UC: Communication Unit (cf. § envelope architecture).

UI: Interface Unit (cf. § envelope architecture).

UT: Processing Unit (cf. § envelope architecture).

4 Envelope Architecture

This document proposes an "envelope architecture" of a Level 1 control system. This envelope architecture is shown in Figure B-2. It covers most of the control systems which can be found presently on the market (see Section 8).

A Level 1 control system can be represented as a set of programmable controllers:

- interconnected through:
  - one or several unit networks, and/or
  - direct I/Os.
- connected to one (or several) Level 2 systems through:
  - one or several unit networks, and/or
  - in the case of conventional control means, direct I/Os.
- connected to the process through:
  - direct I/Os, and/or
  - field buses.
- connected to other Level 1 system through:
  - direct I/Os, and/or
  - communication networks (field buses or unit networks).
- connected to one or several Level 1 Human Machine Interface (HMI) through a dedicated link.

These programmable controllers can be part of a distributed control system (DCS), or independent controllers, such as, for example, a set of independent controllers used in multiple channels of a safety system.

The unit networks link the programmable controllers with other programmable controllers, or Level 2 systems, or other Level 1 systems. They can be separated or merged in a single network.

Typically Level 1 HMI are individual command/setpoint stations or programming and maintenance consoles. Depending on the type of system, the Level 1 programming station will therefore be either a Level 1 HMI or a part of the Level 2 system (normally the case with a DCS).

In this envelope architecture, each programmable controller is composed of:

- a main rack housing one processing unit (UT_1), communication units (UC_0 and UC_1) and possibly interface units (UI) and special units
- extension rack(s) to house additional interface units
- an inter-rack network or extension bus between the main rack and the extension rack(s)
- a range of interface units (UI), such as digital and analog I/O cards, and network communication cards (Modbus, FIP, Hart, Bitbus, etc.), (this document does not address counter modules)
- a processing unit (UT_1), made of one or several modules, and installed in the main rack
- one or several communication unit(s) (UC_0), to interface the programmable controller to one or several unit networks, and installed in the main rack
- one communication unit (UC_1), to interface the main rack with the extension rack(s), and installed in the main rack
- one communication unit (UC_2), installed on each extension rack, to interface this one with the main rack
- one processing unit (UT_2) installed on each of the extension racks
- all power supplies necessary for the operation of the programmable controllers

In order to take into account the possible system redundancies, the different components of this system can be multiplied by two or even by three in the case of safety controllers.

It is intended that any particular system to be tested can be deduced from this envelope architecture by deletion or combination of the components (processing units, communication units, etc.) of this envelope architecture. For instance, the UC_0, UC_1, and UT_1 could belong to the card, as could the UC_2 and UT_2, the main rack may not house any interface unit, main rack and extension rack(s) could be identical (and the inter-rack network or extension bus be absent), etc.

NOTE: For the purpose of timetagging tests, the system is assumed to be connected to an external reference clock which delivers to the system:

- data messages, and/or
- sync pulses.

Several types of synchronization are envisioned here:

- the external reference clock delivers periodically a date message, as well as sync. pulses,
- the external reference clock delivers periodically only a date message,
- the external reference clock delivers periodically sync. pulses, the date being tuned by the operator (through the Level 2 system, or through a Level 1 HMI).

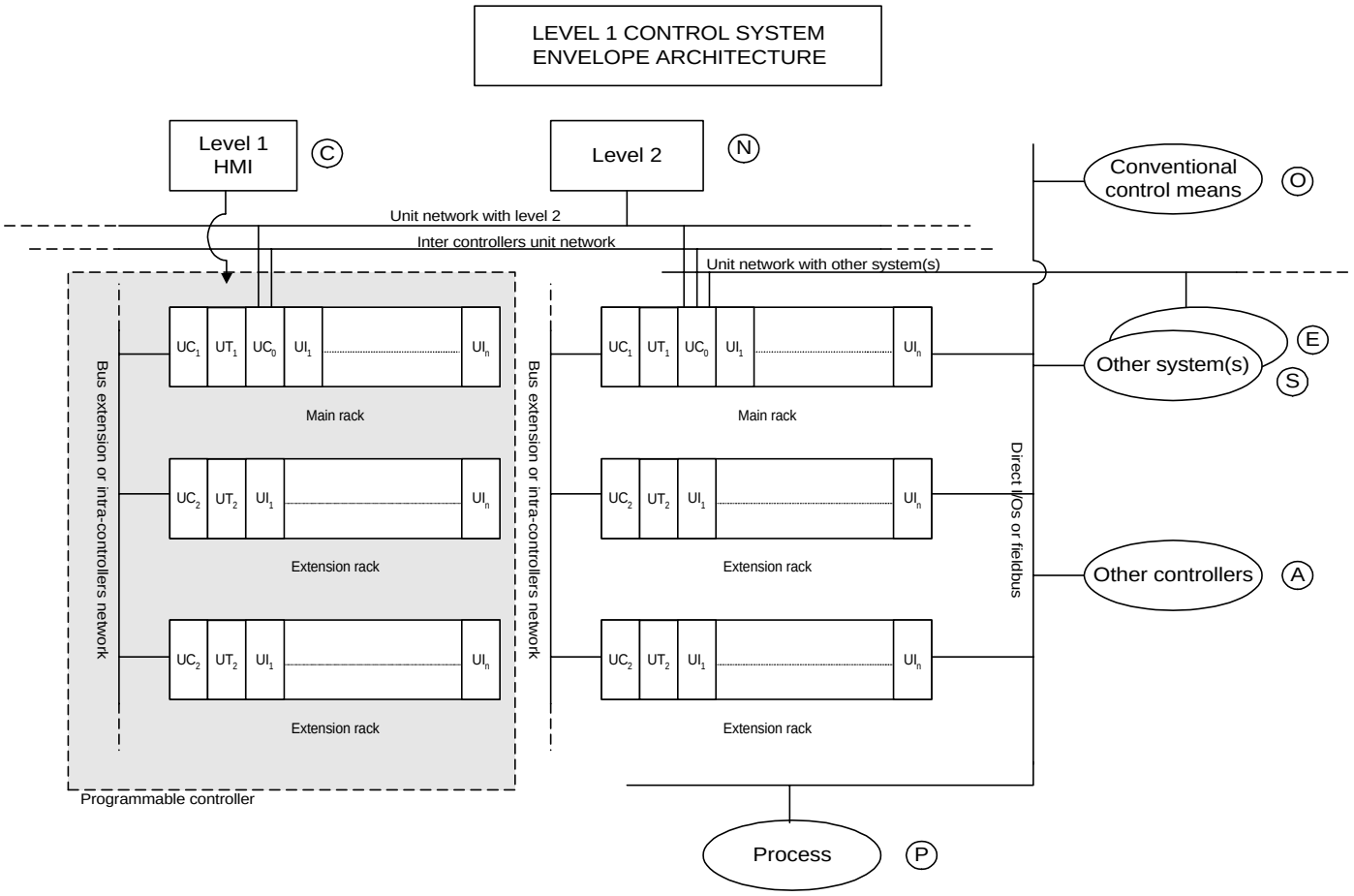


Figure B-2. Level 1 Control System Envelope Architecture

5 Information Transit Time

5.1 How to Use this Document in the Different Steps of the Test Preparation and Execution

The different steps of the evaluation process, leading to the writing of the test program and to the test execution are summarized in Figure B-3. The present document gives principles and recommendations for these various steps:

- Definition of the system to be assessed or qualified, of its architecture, of its interfaces, and comparison with the envelope architecture proposed in Section 4,
- Characterization of the requirements (Section 5.3.2), starting from the requirements identified beforehand (Section 5.3.1),

- Selection of the different paths to be tested (Section 5.3.3),
- System modeling (Section 5.4),
- Selection of the influencing parameters to be tested (Section 5.4.7),
- Selection of the influencing conditions to be tested (Section 5.5),
- Breakdown of the test into sub-tests (Section 5.7.1),
- Definition of the system under test and of the test system (Sections 5.7.2.1 and 5.7.2.2),
- Sub-tests execution and readings (Section 5.7.3),
- Test results analysis and comparison with the system modeling results (Section 5.7.4).

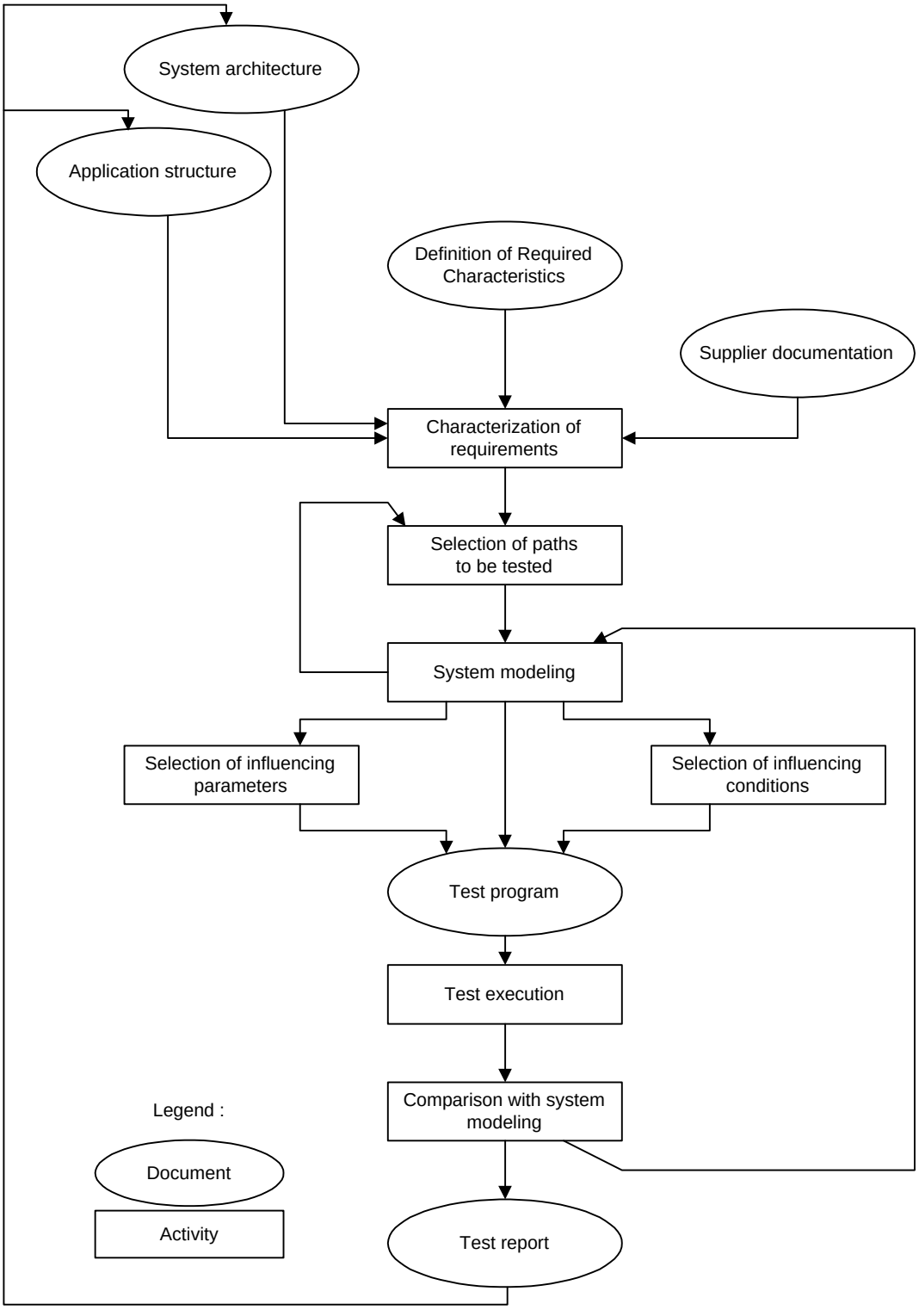


Figure B-3. Transit Time Test Preparation and Execution Process

5.2 Test Objectives

The prime objective of this test is to evaluate globally and in detail the behavior and the performance of the control system with respect to the transit time of information within the system.

The various types of information that are of concern are:

- the system inputs and outputs from and to the process,
- the commands sent or the information received by the operator in the control room, through computer-based workstations or conventional means,
- messages exchanged with other systems through communication networks.

The present test does not address information on the system health or status (e.g., broken wires, power loss, self-diagnostic data, etc.). This type of information and the related performance characteristics are addressed in another investigation group (system maintenance, degraded modes, etc.).

It is important to be able to explain the information transit times measured on a certain number of paths, based on knowledge of the system's data transfer and processing mechanisms. Therefore, one of the objectives of the test is to compare the results obtained from system modeling with the measures collected during the test to understand and master the system's internal mechanisms.

During a qualification process, another objective assigned to the test is the formal demonstration that the system complies with the requirements related to transit time, as expressed in the requirements specification.

During an assessment process, this objective will be limited to checking that the transit times measured are compliant with the typical requirements for control systems to be used in nuclear power plants.

Finally, the test shall supply technical information which is reliable, repeatable, and traceable, and which will:

- support the system evaluation process, giving the acquired level of confidence,
- provide guidance on how to structure future application programs,
- provide guidance on the control system architecture,
- feed the next phases of the control system qualification process.

5.3 Requirements

5.3.1 Typical Requirements on Service Functions

The present chapter proposes a set of typical requirements which can be verified directly or indirectly by the information transit times test. It is a guide for the preparation of the test. The person in charge of the preparation of the test will make sure, through the thorough reading of the requirements specification, that all related requirements have been identified.

In the case of the REP 2000 qualification process, this action is normally performed during the establishment of the characteristics to be verified.

In the case of a system assessment, the reading of this chapter may help the person in charge of the preparation of the test to better identify the purpose of the test, and therefore help him/her to properly structure the test.

Among the typical requirements which are presented here, there are:

- Some which are directly verified. For example, the time response of a safety interlock is explicitly verified during the test.
- Others which are only partially verified. For example, the modulating loop control response time is only partially covered by the transit times test; so is the response time from a Level 2 order to the process.

These typical requirements apply on the following characteristics:

- **Exchanges with a computer-based control room or operator workstation**
  - — Transmission time of an analog order from an operator station

    Actuator output, setpoint,...
  - — Transmission time of a pulse order from an operator station

    Actuator output, setpoint,...
  - — Transmission time of a logic order from an operator station

    Logic output, auto/manual order, ...
  - — Transmission time of an analog information to an operator station

    High level, low level, thermocouple, actuator position, ...

— Transmission time of an logic information to an operator station

Direct logic input, discrepancy, TTL, ...

— Transmission time of an alarm information to an operator station

Alarm generation delay on logic or analog event

- **Exchanges with other Level 1 systems**

— Transfer time of an analog information to another Level 1 system

Information to the turbine governing system, ...

— Transfer time of an logic information to another Level 1 system

Orders sent to the turbine governing system, ...

— Transfer time of an analog information from another Level 1 system

Information from reactor protection system, ...

— Transfer time of an logic information from another Level 1 system

- **Exchanges within the Level 1 system**

— Transfer times of analog information with another controller

— Transfer times of logic information with the same controller

— Transfer times of analog information between two controllers

— Transfer times of logic information between two controllers

— Transfer times of analog information between two channels

— Transfer times of logic information between two channels

— Transfer times of analog information between 1E and non-1E systems

— Transfer times of logic information between 1E and non-1E systems

- **Modulating and sequential control**
  - Modulating control performances

    Maximum transit times between an analog input, a modulating processing, and an analog output

    Maximum phase difference, PID cut-off frequency
  - Interlock control performances

    Maximum transit times between a logic input, a boolean processing, and a logic output (for any path)

    Maximum transit times between an analog input, a processing, and an analog output (for any path)
  - Protective control performances

    Maximum transit times between a logic input and a logic output
- **Exchanges with other Human Machine Interface**
  - Transmission time of an analog order from an auxiliary control station

    Setpoint, analog output, ...
  - Transmission time of a pulse order from an auxiliary control station

    Setpoint, analog output, ...
  - Transmission time of a logic order from an auxiliary control station
  - Transmission time of an analog information to an auxiliary control station

    Measure, actuator position, ...
  - Transmission time of a logic information to an auxiliary control station

    Direct logic input, discrepancy, TTLE, ...
  - Transmission time of an analog information to mimic panel

    Measure, actuator position, ...

— Transmission time of an logic information to mimic panel

Direct logic input, discrepancy, TTLE, ...

— Transmission time of an analog information from another peripheral system

— Transmission time of a logic information from another peripheral system

— Transmission time of an analog information to another peripheral system

— Transmission time of a logic information to another peripheral system

5.3.2 Characterization of Requirements

The requirements likely to be directly or indirectly verified by the information transit times test, as identified in the previous chapter, need to be characterized, i.e., translated in terms of transit times for a given path.

In this chapter, the studied characteristic (the transit time) is precisely defined, then the different paths within the system are identified: a path is completely defined by its input, its output, the physical trajectory taken by the signal, and the processing performed on this signal.

5.3.2.1 Transit Time Definition

The transit time is defined, for a given path, as the duration between:

- an event on the input of the path:

  — for a direct LOG input: opening or closure of a contact (assumed to be without bounce).

  — for a direct ANA input: significant variation of this variable, i.e., higher than a predefined percentage of the range of this variable, always performed on a duration smaller than the studied response times (one millisecond recommended).

  — for a network input: the event chosen will be either the moment a new value of the input variable is made available in a memory register of the other system, or the moment this new value is sent in a message through the network. The choice between these two moments will depend on the boundaries between the scope of supply of the two systems, on the type of network, and on the technical feasibility of the detection of this moment.

- and the corresponding event on the output of the path, i.e.,:
  - for a direct LOG output: opening or closure of the output card contact.
  - for a direct ANA output: variation higher than a predefined percentage of the total variation due after the event on the input.

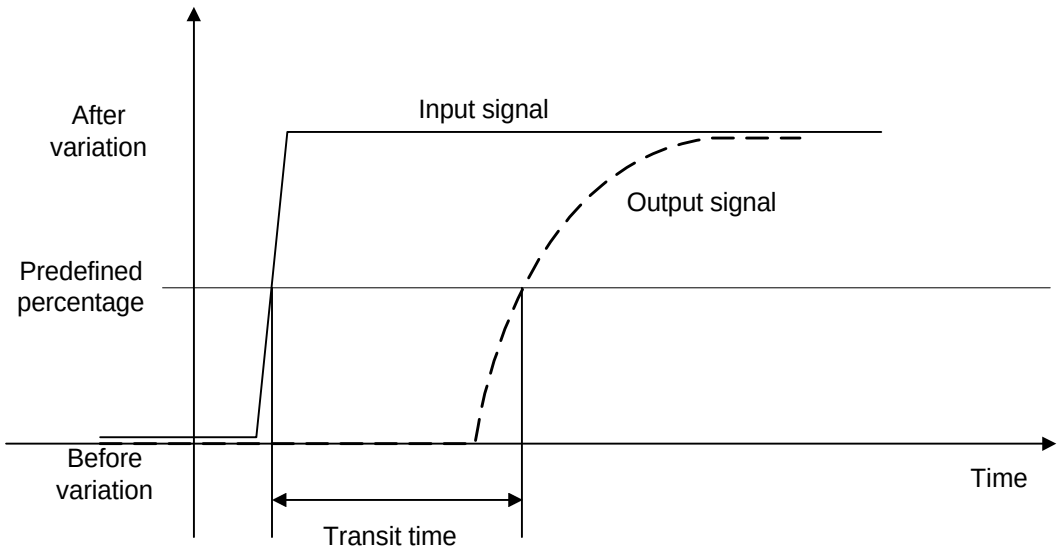


Figure B-4

  - for a network output: the event will be chosen between on the moment the new value of the output variable is made available to the other system in a memory register, or the moment this new value is sent in a message through the network. As for the inputs, the choice between these two moments will depend on the limits of supply between the two systems, on the type of network, and on the technical feasibility of the detection of this moment. In the case of ANA network output, the same predefined percentage of variation than for ANA direct output shall apply.

The value of the variation applied at the input of the system, as well as the predefined percentage used to measure the transit time, will depend on the path to be tested.

For both LOG and ANA variables, transit times may depend on the type of transition (up or down) selected for the input. Therefore the type of transition will be selected once and for all, taking the one which gives the highest transit times.

5.3.2.2 Paths

A path represents the route taken by a signal, and is characterized by:

- its input and its output at the borders of the system,
- the physical trajectory taken by the signal (type of input card; set of processing units, communication unit, and networks used; type of output card), and
- the type of processing performed on this signal (systematic or application): see definition in 5.3.2.2.3.

5.3.2.2.1 The System Inputs and Outputs

Systems Connected	I_{LOG}	O_{LOG}	I_{ANA}	O_{ANA}
Level 2 system	N1	N2	N3	N4
Level 1 HMI	C1	C2	C3	C4
Other systems (connected through unit network)	E1	E2	E3	E4
Process, conventional control means, other controllers or other system (P, O, A, or S)				
- Direct I/Os	X1	X2	X3	X4
- Fieldbus I/Os	X'1	X'2	X'3	X'4

5.3.2.2.2 Physical Trajectories

Based on the envelope architecture identified in the previous chapter, there are many possible paths, which can be structured around all the possible combinations of I/Os types.

- [X↔X] Between conventional control means, process, other systems, or other controllers, the different trajectories are obtained by selecting:

  - whether the input and output belong to the different controllers, or belong to the same controller but not to the same rack, or belong to the same rack but not to the same interface unit, or belong to the same interface unit,
  - the types of the two interface units.

- [N↔X] Between a Level 2 system and conventional control means, process, other systems, or other controllers, the different trajectories are obtained by selecting:
  - whether the interface unit is on the main rack or on an extension rack,
  - the type of the interface unit.

- [E↔X] Between conventional control means, process, other systems, or other controllers and other systems, the different trajectories are obtained by selecting:
  - whether the interface unit is on the main rack or on an extension rack,
  - whether the controller containing the unit interface is directly connected to the other system or not,
  - the type of the interface unit.

- [C↔X] Between a Level 1 HMI and conventional control means, process, other systems, or other controllers, the different trajectories are obtained by selecting:
  - whether the interface unit is on the main rack or on an extension rack,
  - whether the input and the output belong to the same controller or not,
  - the type of the interface unit.

- [N↔N] Between two Level 2 systems, the different trajectories are obtained by selecting:
  - whether the two Level 2 systems are distinct or not.

- [E↔N] Between a Level 2 system, and another system, the different trajectories are obtained by selecting:
  - whether the Level 2 system and the other system belongs to the same network or not.

- [C↔N] Between a Level 2 system and a Level 1 HMI, there is only one possible trajectory.

- [E↔E] Between 2 other systems, the different trajectories are obtained by selecting:

  — whether these other systems are distinct and belong to different network, are distinct and belongs to the same network, or are not distinct.

- [C↔E] Between a Level 1 HMI and another system, , the different trajectories are obtained by selecting:

  — whether the controller to which the Level 1 HMI is connected, is directly connected to the other system or not.

- [C↔C] Between two Level 1 HMI, the different trajectories are obtained by selecting:

  — whether the two Level 1 HMI are distinct and connected to two different controllers, are distinct and connected to the same controller, or are not distinct.

5.3.2.2.3 Processing

Processing performed on a signal can be divided into two categories, the systematic processing, and the application processing:

- systematic processing is the system or pre-programmed (configurable or not) processing which is potentially performed on all variables of the same kind (A/D conversion, filtering, chattering processing, etc.)

- application processing is the programmed processing, adapted per variable.

Systematic processing shall always be performed on the paths subject to tests.

Application processing performed on the paths subject to tests shall be the following:

- a minimum logic processing,

- a minimum analog processing,

- a minimum mixed processing enabling the conversion of an ANA input into an LOG output and vice versa.

The application processing will be chosen as simple as possible and therefore can be considered as the fastest.

As a general rule:

- the minimum logic or analog processing will be: Output = Input.
- the mixed processing will be:
  - f(ANA) = 0 if ANA < threshold and f(ANA) = 1 if ANA > threshold (without dead band)
  - g(TOR) = ANA1 if TOR = 0 and g(TOR) = ANA2 if TOR = 1

The application processing selected may be reviewed after the system modeling step, if it appears that:

- some application processing use specific components or operation modes (e.g., special modules),
- or the minimum application processing selected is not representative of the normal system elementary tasks precedence, due to its simplicity.

5.3.3 Selection of the Paths to be Tested

The mere reading of the previous chapter highlights the necessity to select the paths which will be subject to test. This selection will be made on the basis of the following criteria:

- requirements expressed in the requirements specification (if any),
- time and resources constraints,
- foreseen system architecture and application structure to be assessed or qualified,
- data available through other analysis and tests means (e.g., review of experience, supplier's data, etc.).

This selection may be revised or improved when the results of the system modeling or of the first sub-tests are available.

As a general rule, the paths which are most likely to be tested are the following:

Path	Input	Trajectory	Application Processing	Output
"simple logic" between two controllers	X1	[XX]: X1 and X2 belong to different controllers	Minimum logic processing	X2
"simple logic" within a controller	X1	[XX]: X1 and X2 belong to the same controller	Minimum logic processing	X2
"simple analog" between two controllers	X3	[XX]: X1 and X2 belong to different controllers	Minimum analog processing	X4
"simple analog" within a controller	X3	[XX]: X1 and X2 belong to the same controller	Minimum analog processing	X4
Logic information to Level 2	X1	[NX]: X on extension rack	Minimum logic processing	N2
Logic order from Level 2	N1	[NX]: X on extension rack	Minimum logic processing	X2
Analog information to Level 2	X3	[NX]: X on extension rack	Minimum analog processing	N4
Analog order from Level 2	N3	[NX]: X on extension rack	Minimum analog processing	X4

Some of these paths may be considered as secondary. It means that they are intended to cover only a part of a system set of processing, and the corresponding sub-tests will be less complete than for the other paths.

5.4 System Modeling

5.4.1 Objectives

The objectives of the system modeling are:

- identification of the influencing conditions whose impact on the transit times will be measured,
- computation of theoretical maximum and minimum transit times, as a function of these influencing parameters, for future comparison with the results of the transit times measures,
- identification of potentially difficult points, which shall be subject to particular attention during the test preparation or execution.

5.4.2 Method

The system modeling shall observe the following steps:

- identification of the technical functions used,
- breakdown of the different paths into technical functions,
- determination of the technical functions characteristics, as a function of the influencing parameters,
- consolidation of these characteristics for each path, as a function of the influencing parameters,
- selection of the influencing parameters (and their set of values) subject to measure.

5.4.3 Technical Functions

The main technical functions to be modeled are:

- A/D conversion,
- acquisition scanning,
- filtering,
- chattering processing,

- validity status management,
- grouping of variables for transmission,
- variables network transmission,
- minimum application processing.

5.4.4 Paths Breakdown

The paths selected previously (Section 5.3.3) shall be broken down into a succession of technical functions.

5.4.5 Technical Functions Characteristics

5.4.5.1 Technical functions characteristics

The following characteristics of the technical functions shall be described:

- function activation mode: periodic, synchronized with preceding function, using semaphore, synchronized with the parallel function in case of a normal/backup operation (including voting mechanisms for the safety controllers),
- periodicity (if applicable),
- duration,
- priority; interruptibility; behavior in case of interrupts.

Networks will be handled as technical functions (transmission function).

The above elementary characteristics may vary with the system influencing parameters. They will be subject of a first consolidation, in order to establish for each technical function:

- waiting and execution minimum times,
- waiting and execution maximum times,

which will generally be a function of the system influencing parameters.

5.4.5.2 (System) Influencing Parameters

The system influencing parameters (or simply the influencing parameters) are the system parameters which are configurable for the purpose of a particular application, and which are likely to influence the information transit times of the system. They are mainly:

- UT and UC cycle times,
- acquisition and emission rates,
- systematic processing parametering (dynamic filtering, static filtering, chattering processing, time tagging, etc.),
- redundancy level of the different UT, UC, and networks,
- tasks priority,
- size and complexity of the application program and database, represented in a simplified manner by an artificial UT load,
- number of I/Os used per interface unit,
- number and types of cards per rack,
- number of racks and cards per controller,
- number of controllers, racks and cards per system.

5.4.6 Consolidation

Based on the breakdown of paths into technical functions, and the characterization of these technical functions, a consolidation of the following characteristics shall be performed for each of the selected paths:

- a maximum transit time,
- a minimum transit time,

as functions of the influencing parameters.

5.4.7 Selection of The Influencing Parameters

The system influencing parameters, and their associated set of values (for a given influencing parameters, one or several values may be chosen at this point of time),

which will be used to defined the different measures (cf. definition in §12.1) will be selected on the basis of the following criteria:

- system architecture to be qualified or assessed,
- importance of the influence.

5.5 Influencing Conditions

Among all possible influencing conditions as identified in the [1069] standard, those likely to have an actual impact on the information transit times are the following:

- system tasks: on-line application modification, operation in degraded mode, on-line module insertion,
- personal: access to the system using the Level 1 HMI,
- process: I/Os flow variation,
- utilities: disturbances on the power supply,
- environment: electromagnetic disturbances,
- available services: without influence,
- other systems linked to the system: network load (with Level 2, with other systems).

The influencing conditions such as "I/Os flow variation" are handled in the "System behaviour under process avalanche" investigation group, and not in the "performance" investigation group.

The influencing conditions such as "utilities" and "environment" are handled in the "Environment" investigation group, and not in the "Performance" investigation group.

Therefore, the influencing conditions which will be considered to define the different measures within the present information transit times test are the following:

- system operation with the loss of an UT, an UC, an UI, a network or a fieldbus (if the system configuration enables such an operation),
- module (UT, UC, UI) on-line extraction and reinsertion,
- on-line system application modification and loading,
- operator intervention on the maintenance/programming console,

- load of the different networks.

The selection of the different influencing conditions which will be subject to measures will be based on the following criteria:

- requirements expressed in the requirements specification (if any),
- time and resources constraints,
- data available through other analysis and tests means (e.g., return of experience, supplier's data).

The influence of these conditions may be measured on a limited number of paths among the selected ones.

5.6 Documentation Required for the Test

The documents required in order to start the test program are the following:

- the present document,
- a document (e.g., Quality Plan) describing the Quality arrangements taken for the test, covering at least the following points:
  - responsibilities and competence of the persons in charge of test preparation and execution,
  - documentation management,
  - planning and progress control,
  - modification and configuration management (of the system under test and the test system).
- the supplier documentation, which shall:
  - correspond to the version of the system being tested,
  - enable a first system modeling.
- the architecture of the system to be assessed or qualified
- the application structure (if available)

- the complete set of requirements likely to be directly or indirectly verified by the information transit times test. These requirements:

  — may be either directly available in the form of a referential of characteristics, containing the sub-set of requirements which need to be verified during the information transit times test in the evaluation phase of the support system, or

  — may need an extraction from a document specifying generic requirements.

5.7 Test Description

5.7.1 Test Organization

The subject is to measure information transit times on the different selected paths (Section 5.3.3), and with varying selected influencing parameters and conditions (Sections 5.4.7 and 5.5).

The information transit times test is first broken down into several sub-tests, each sub-test corresponding with a given pre-selected path.

Then each sub-test may be broken down into several measures, each measure corresponding to a given set of influencing parameters and conditions.

Each measure may be further broken down into several repetitions, each repetition being separated from the previous one by either a power supply interruption, or by a processing units re-initialization.

Suggested number of repetitions for each measure is 4, but this figure shall be confirmed in the test program. It may be:

- increased if the first repetitions indicate an important transit times standard deviation or unexplainable values, or
- decreased for secondary paths, or
- decreased if the first repetition results match with the system modeling.

Finally, each repetition is made of an important number of samples, each sample corresponding to an elementary transit times reading.

Suggested number of samples for each repetition is 500, but this figure shall be confirmed in the test program. It may be:

- increased if the first samples indicate an important transit times standard deviation or unexplainable values, or
- decreased for secondary paths, or
- decreased when the path input stimulation, or the path output detection, cannot be automated (as in the case of HMI I/Os).

Time distance between two samples shall be chosen at random.

5.7.2 Configurations

5.7.2.1 System Under Test

Configuration of the system under test shall be such as it enables to test all the selected paths (however not necessarily at the same time). The preferred paths, as identified in Section 5.3.3, lead to the definition of the following minimal configuration:

- Two programmable controllers, equipped each with:
  - 1 main rack, with its processing unit (UT1), and its two communication units (UC0 and UC1)
  - 1 extension rack, with its processing unit (UT2), and its communication unit (UC2)
  - its bus extension or intra-controller network
  - its power supply
- a set of interface units (UI), containing two UI of each type, and in sufficient quantity to ensure that the influencing parameters (such as number of cards per rack) as defined during the system modeling phase are properly represented,
- one maintenance/programming console,
- the level HMI, if any,
- the inter-controller unit network, with the 2 controllers as its subscribers
- the unit network with Level 2,
- the unit network(s) with the other systems (if any),

- the means to simulate the loads of the various networks, when these loads have been identified as possible influencing conditions.

The redundancy level of each component will be the one of the architecture to be qualified or assessed.

5.7.2.2 Test System

The test system shall enable:

- on one side, to stimulate the inputs of all paths selected for the test:
  - direct LOG input
  - direct ANA input
  - network input (fieldbus, network with other systems, network with Level 2 system)
  - Level 1 HMI input
- on the other side, to monitor and record variation of the outputs of all paths selected for the test:
  - direct LOG output
  - direct ANA output
  - network output (fieldbus, network with other systems, network with Level 2 system)
  - Level 1 HMI output

For this purpose, one or more signal generators and a signal recorder shall be used.

5.7.2.2.1 Signal Generator(s)

The signal generator(s) shall be capable to perform the following functions:

- for the LOG inputs: generation of dynamic square signals, in random sequence,
- for the ANA inputs: generation of voltage or current signals, covering the complete electrical range, and of various shapes (square, ramps, sinusoidal waveform),

- for the network inputs: the choice of the equipment (emulator, ...) will depend on the limit chosen to measure the event (availability in a memory register, or transfer of the corresponding message over the network: Section 5.3.2.2.1),
- for the Level 1 HMI inputs: the inputs cannot be automatically stimulated, and shall be changed manually.

5.7.2.2.2 Signal Recorder

The signal recorder shall be capable to:

- record the input signal,
- record the output signal (LOG or ANA; direct or network),
- compute the time elapsed between the event on the input, and the corresponding event on the output, with a precision equal or better than one millisecond,
- keep track (in writing as well as in a standard computer format) of the measures, in order to ensure the test traceability and reproducibility.

5.7.3 Measures Description

Each repetition consists in:

- injecting to the path input the following signal:

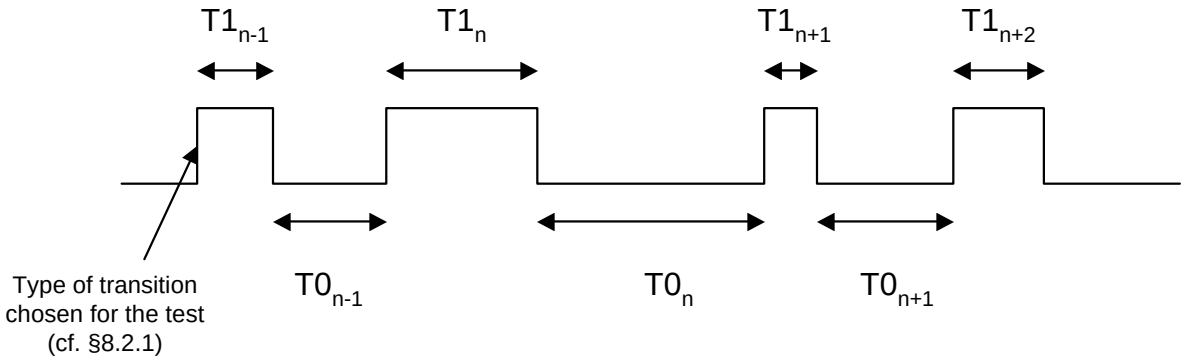


Figure B-5

where $T1_n$ is chosen at random, and where $T0_n$ is chosen high enough to always be longer than the longest transit times likely to be measured during the sub-test, and to never generate loss of information,

- recording the two signals (injected on the path input, and available on the corresponding path output), in order to enable a qualitative analysis of the shape of the output signal,
- computing the time difference between the event on the path input, and the event on the path output.

The following readings or computations shall be recorded:

- for each sample : an elementary transit time
- for each repetition:
  - a minimum transit time
  - a maximum transit time
  - an average transit time
  - a standard deviation
  - a curve (sample n°, transit times)
- for each measure:
  - a minimum transit time
  - a maximum transit time
  - an average transit time
  - a standard deviation

5.7.4 Analysis and Comparison with the System Modeling

The analysis of the above recordings shall cover for each measure:

- comparison of transit times (minimum, maximum, and distribution) obtained during the test with those obtained by the system modeling, and verification of the impact of the influencing conditions on the transit times,
- identification of transit times which cannot be explained by the system modeling,
- identification of influencing conditions having a significant impact on the transit times.

These analysis shall enable the confirmation of the system modeling, after possible modifications of this modeling and consultations with the system supplier.

5.8 Expected Results

The results expected from this test are of various natures, depending on the objectives this test fulfills:

- To understand and master the system, the test should insure:
  - the validation of the system modeling
  - the validation of the system supplier data
  - the detection of possible system operation anomalies
- To guide the system realization, the test should supply:
  - recommendations for the architecture design
  - recommendations for the system configuration
- To continue the system qualification (when applicable), the test should supply:
  - recommendations for possible additional analysis or simulation required to complete the (Level 1) control system evaluation
  - recommendations for possible additional analysis or simulation required to complete the overall control system or the other systems evaluation
  - a list of additional information required from the supplier
- To formally demonstrate the fulfillment of the requirements related to the information transit time (as long as the recommendations given on the system architecture or configuration are followed), the test should confirm:
  - the maximum, minimum and average transit times
  - the main influencing parameters and conditions, and their impact on the transit times

6 System Behavior During An Avalanche

6.1 How to Use this Document in the Different Steps of the Test Preparation and Execution

The different steps of the evaluation process, leading to the definition of the test program and to the test execution are summarized in Figure B-6. The present document gives principles and recommendations for these various steps:

- Definition of the system to be assessed or qualified, of its architecture, of its interfaces, and comparison with the envelope architecture proposed in Section 4,
- System modeling (Section 6.5),
- Selection of the influencing parameters to be tested (Section 6.5.5.2),
- Execution of the first phase of the test, (Section 6.8.3),
- Characterization of the requirements (Section 6.4.2), based on the requirements identified beforehand (Section 6.4.1), leading to:
  - selection of the different system missions to be validated during an avalanche (Section 6.4.2.1)
  - selection of the avalanche profiles (Section 6.4.2.2), and of the rules to simulate the avalanche on the system inputs (Section 6.4.2.3)
- Selection of the influencing conditions to be tested (Section 6.6),
- Execution of the second phase of the test, (Section 6.8.4),
- Execution of the third phase of the test, (Section 6.8.5),
- Test results analysis and test reports (Section 6.9).

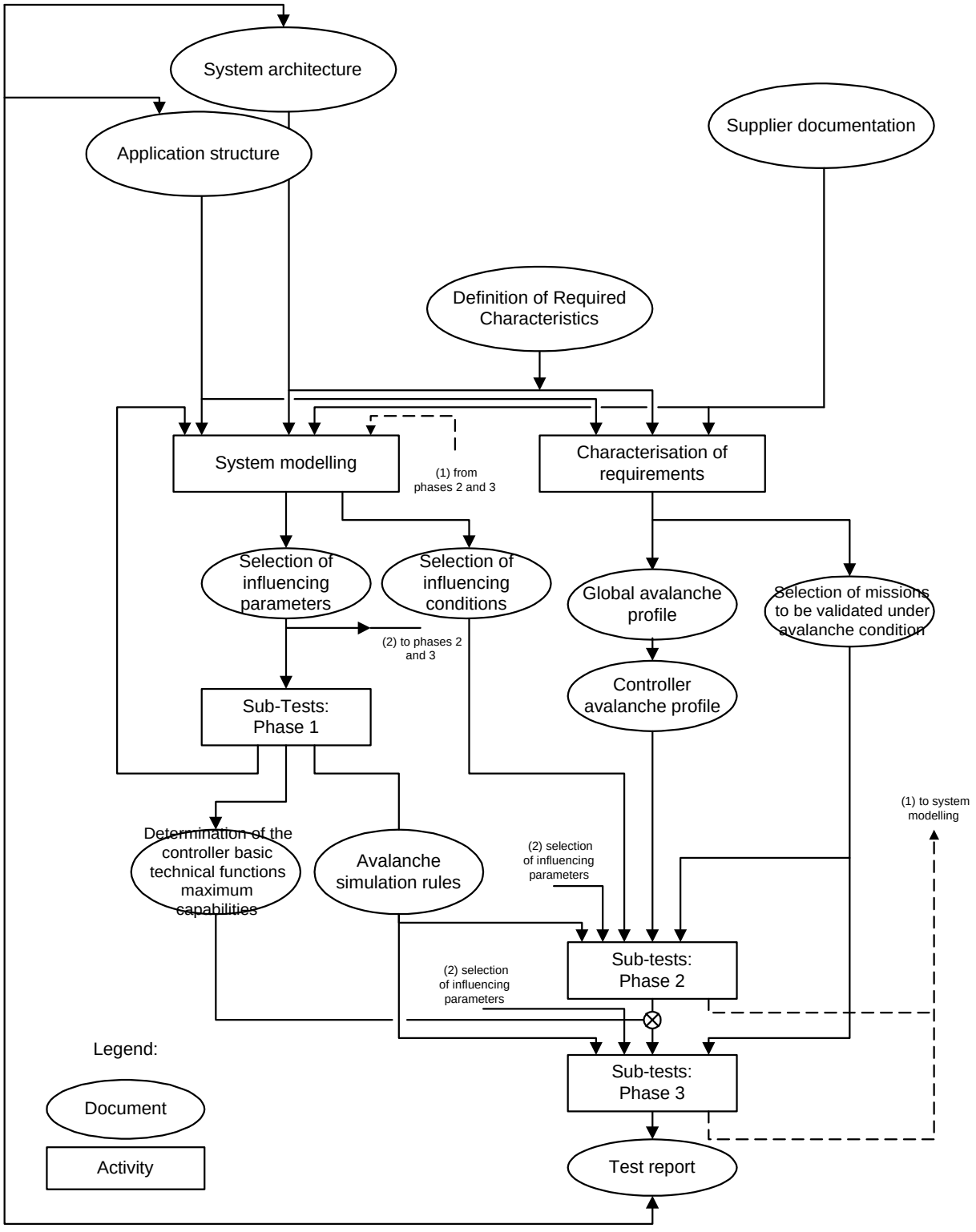


Figure B-6. System Behavior During an Avalanche Test Preparation and Execution Process

6.2 Test Objective

The prime objective of this test is to evaluate globally and in detail the behavior and the performance of the system during the occurrence of a process avalanche, i.e., a burst of events.

- The first point is to understand the system mechanisms involved in information transmission and processing.
- The next point is to evaluate the influence of an important flow of information on the execution of these mechanisms.
- Another point is to demonstrate that, provided certain precautions (which need to be detailed by the test) are taken, the system complies with the expressed requirements, even during an avalanche.
- The last point is to evaluate the margin available above the contractual or typical avalanche, by defining a maximum avalanche profile (i.e., a boundary avalanche), above which the system does not fulfill its requested missions.

In case of a system qualification, the test shall lead to the formal demonstration that the requirements expressed in the requirements specification are met. Typical requirements are the preservation (or a maximum authorized deterioration) of given missions, or the information made available to the operator during the occurrence of an avalanche. They should be preceded by a definition of contractual or typical avalanche profile.

In case of system assessment, the test shall lead to the validation of the system behavior and performances, taking into account the avalanche profile definition and the missions proposed in the present document.

Finally, the test shall supply technical information which is reliable, repeatable, and traceable, which will:

- enable the pursuit of the system evaluation process, based on the level of confidence acquired,
- provide guidance on how to structure the future application programs,
- provide guidance on how to build the control system architecture,
- feed the next phases of the control system qualification process,
- enable to estimate the margin available with the maximum avalanche the system can process.

6.3 The Different Phases of the Test

6.3.1 Phase 1: Behavior of the System basic Technical Functions during an Avalanche

The purpose of this first phase is to analyze the basic transmission and processing mechanisms within the system. It is intended to understand the different system components, and their basic technical functions:

- interface units (UI): scanning, filtering, FIFO management, overflow management,
- processing units (UT): tasks management, priority management, overload management,
- communication units (UC): flows, overflow management, transfer to other systems, ...

This phase does not address application processing.

The objectives of this phase are:

- to complete and validate the system model, by comparing the results obtained by the system modeling, with those obtained during this test phase.
- to identify the origins and conditions of possible system locking, as well as the information transfer or processing limits of the controller basic technical functions.
- to understand the events transmission mechanism within the system, in order to properly define the avalanche simulation rules for the next phases of the test. This objective is compulsory, because that avalanches used the phases 2 and 3 are simulated by triggering a limited number of the system inputs, hence requiring to justify their representativeness.

6.3.2 Phase 2: Behavior of the System Functions During a Typical or Contractual Avalanche

This second phase of the test is directed towards the system behavior during an avalanche based on an operator point of view. This approach consists to evaluate the behavior and the performances of a few typical functions during an avalanche. The system functions considered for this phase are:

- a PID modulating loop,
- a transfer of information from the process,

- an automatic logic control,
- a manual control from Level 2 system,
- a manual control from Level 1 auxiliary conventional control means,
- time tagging.

These functions and the corresponding test may be completed after further investigation, depending on requirements expressed in the requirements specification.

The avalanche used to carry out this phase is the contractual one (in case of a system qualification), or a typical one (in case of system assessment). In order to perform this phase of the test, it is therefore necessary:

- that a global (i.e., applicable to the complete Level 1 system) contractual or typical avalanche profile does exist, and
- that a controller (i.e., applicable to a single controller) avalanche profile can be deduced from this global avalanche profile.

If such controller avalanche profile cannot be obtained, then phase 2 of the test shall be skipped, and possibly performed later on during the project when this controller profile can be determined.

The objectives of this second phase of the test are:

- to formally demonstrate the proper execution and performances of the retained system functions,
- to verify the information made available to the operator,
- to assess the system internal behavior (system load, impact of the avalanche on the parts of the system not concerned by the avalanche),

when the system is subject to the contractual or typical avalanche, and then to verify that the system is fully back into normal operation after the avalanche is absorbed.

6.3.3 Phase 3: Determination of the Boundary Avalanche

The purpose of this third and last phase of the test is to determine the boundary avalanche, so as to evaluate the margin available between the contractual or typical avalanche, and the boundary avalanche above which the first losses of system missions appear. The approach is:

- if phase 2 of the test has been carried out : to increase the contractual or typical avalanche profile used during this phase 2, up to the point where the system ceases to perform its missions,
- if phase 2 of the test has not been carried out : to start with an avalanche profile based on the maximum events flows manageable by the system basic technical functions (as identified during the phase 1), and to decrease this profile up to the point where all the system missions are restored.

The notion of “loss of the system missions” shall be properly defined, based on the requirements expressed in the requirements specification.

Another purpose of this third phase is to verify that the system is fully back into normal operation after the boundary avalanche is absorbed.

The objectives of this third phase of the test are:

- to provide system configuration rules required to guarantee that the expressed requirements will be met when the system is subject to an avalanche.
- determine the margin available between the contractual or typical avalanche, and the boundary avalanche above which the system missions are lost or degraded above predefined acceptable levels.

6.4 Requirements

6.4.1 Typical Requirements on Service Functions

The present chapter proposes a set of typical requirements which can be verified directly or indirectly by the "system behavior during an avalanche" test. It is a guide for the preparation of the test. The person in charge of the preparation of the test will make sure, by reading thoroughly the requirements specification, that all related requirements have been identified.

In the case of the REP 2000 qualification process, this action is normally performed during the establishment of the referential of characteristics.

In the case of a system assessment, the reading of this chapter may help the person in charge of the preparation of the test to better identify the purpose of the test, and therefore help him to properly structure the test.

These typical requirements apply on the following characteristics:

- **Preservation of a given mission during the occurrence of an avalanche**
  - acquisition, processing and transfer of LOG and ANA process information,
  - time tagging
  - modulating control: bumpless, and without loss of control
  - auto/manual change over
- **Authorized deterioration of a given mission during the occurrence of an avalanche**
  - maximum authorized delay of a LOG or ANA information transmission times
  - maximum overall time necessary to process all the events of an avalanche
  - maximum authorized suspension period of certain missions
- **System load during the occurrence of an avalanche**
  - maximum dynamic overload
  - CPU maximum load
  - non influence of an avalanche on the parts of the system not concerned
- **Information made available to the operator during the occurrence of an avalanche**
  - buffer saturation on system components
  - CPU overload
  - task non execution
- **Content of supplier documentation**
  - flow capacity of each system component
  - component behavior when saturated

— list and size of buffers

— maximum flows manageable by the different buses and networks

6.4.2 Characterization of Requirements

The requirements likely to be verified by the "system behavior during an avalanche" test, as identified in the previous chapter, need to be characterized, i.e., the following aspects shall be properly defined:

- the missions whose correct execution and performances will be monitored when the system is subject to an avalanche,
- the contractual (in case of system qualification), or typical (in case of system assessment) avalanche profile,
- the rule to simulate an avalanche on the system (in terms of system inputs, physical trajectories, and processing performed).

6.4.2.1 Determining the System Missions to be Monitored During an Avalanche

By default, the missions chosen, i.e., whose operation and performances (performances chosen being indicated in brackets) will be verified during an avalanche, are the following:

- modulating control, such as a PID loop (response times and accuracy),
- transfer of LOG and ANA process information (response times and accuracy),
- automatic logic control (response times),
- manual (LOG and ANA) control from Level 2 (response times and accuracy),
- manual (LOG and ANA) control from Level 1 HMI (response times and accuracy),
- time tagging (accuracy).

These missions and associated performances may be reviewed depending on the requirements expressed in the specification, as well as on the resources and time schedule constraints.

The notion of "loss of system mission" shall be quantified, i.e., limits shall be defined above which the missions or performances deterioration is no longer acceptable. This definition shall be based on elements such as:

- loss of function integrity:
  - loss of processed information,
  - non execution of a given processing, ...
- or deterioration of function performances:
  - delay in information transfer higher than a predefined limit,
  - accuracy of event time tagging,
  - delay of execution of a given processing higher than a predefined limit,
  - deterioration of a PID loop higher than a given limit, ...

6.4.2.2 Determining the (Global and Controller) Avalanche Profiles

The different types of system inputs are:

- the process inputs (whether direct or through fieldbus),
- the operator inputs (through Level 2 system, or Level 1 HMI),
- the inputs from the other system (through unit networks).

This document assumes that the avalanche cannot originate either from the operator inputs, or (but subject to verification) from the inputs from the other systems.

An avalanche profile can be defined, in a general but simplified manner, as the generation of events (cf. glossary) on LOG and ANA process inputs, according to two curves (one for the events on the LOG inputs, another for the events on the ANA inputs) having the following (not necessarily monotonic) forms:

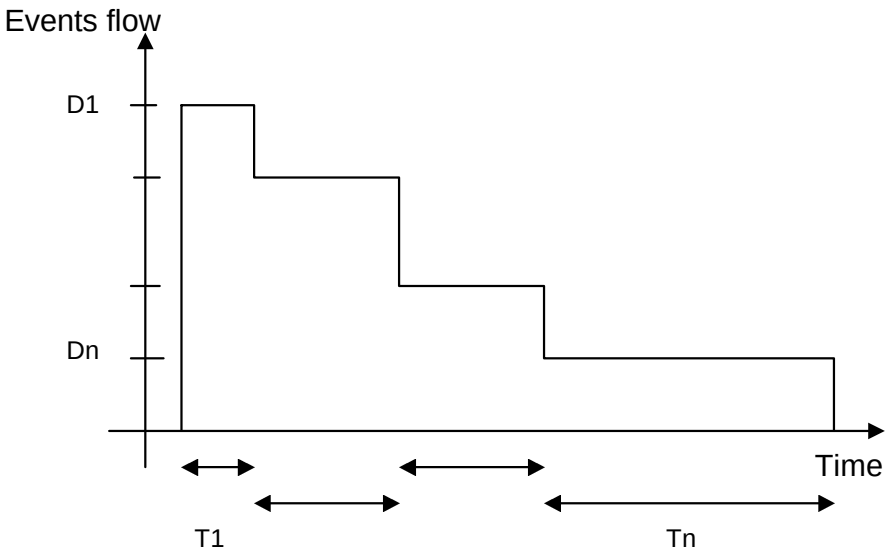


Figure B-7

- In the case of LOG inputs, the flow of events corresponds to a number of changes of state per second.
- In the case of ANA inputs, the flow of events corresponds to a number of variations higher than a predefined dead band taken here by default equal to 0.5%.

This avalanche profile is defined in principle for the complete Level 1 system. In order to perform the phase 2 of the test, it will be compulsory to deduce a controller avalanche profile, i.e., a curve of flow of events generated on a single controller, from this global (contractual or typical) avalanche profile. This operation can originate:

- either directly from the requirements specification, when this one provides a controller avalanche profile,
- or from the configuration of the system under qualification, if such configuration has already been carried out,
- or from a simplifying hypothesis.

6.4.2.3 Determining the Rule to Simulate an Avalanche on the System

The issue is to define the rules which will be followed to simulate an avalanche with a predefined profile on a limited number of inputs, and on a given number of paths.

Each path represents the different routes taken by the events generated on the system inputs, and is characterized by the physical trajectories along which the signal is

transmitted (processing units, communication units, and networks used), and the processing performed on the signal.

For practical reasons, i.e., mainly in order to reduce the size of the system under test, the avalanche will be generated on a limited number of inputs, by periodic triggering of these inputs. This method of generating an avalanche is normally not representative of a real avalanche (where any given input is triggered once, or maximum twice). It is therefore necessary to make sure that this avalanche generation method does not put forward system limitations which are due to the basic technical functions, and would not be relevant in case of a real avalanche.

6.4.2.3.1 System inputs

The issue is to assign the two (LOG and ANA) controller avalanche profiles, as presented in Section 6.4.2.2, on a given number of:

- system inputs,
- interface units,
- racks,

and on a given controller architecture. The minimum configuration will be looked for, with the constraint that the flow generated on any input, interface unit, or rack must stay below the system basic technical functions limitations as identified during the first phase of the test.

6.4.2.3.2 Paths

After the assignment of the avalanche profile on the inputs of the system, it is necessary to describe how these events will be distributed and processed within the system.

In order to simplify the problem, the only paths considered are the ones originating from the process and terminating on the Level 2 system. The paths terminating in other outputs (such as other system, Level 1 HMI, or process) are not addressed.

The paths are characterized using simple ratios between:

- the number of inputs (LOG or ANA)
- the number of outputs towards the Level 2 system, for which an event is generated by an event on one of the inputs

outputs / inputs	I_{LOG}	I_{ANA}
LOG outputs towards Level 2 (N)	100 + l1% [1]	75%
ANA outputs towards Level 2 (N)	0%	100 + a1% [1]

Note [1]: All LOG and ANA inputs are sent to Level 2 system.

6.5 System Modeling

6.5.1 Objectives

The objectives of the system modeling are:

- calculation of the information transmission and processing maximum flows, for each path taken by the avalanche,
- identification of the influencing parameters whose impact on the behavior of the system during an avalanche. In particular, the possible influence of the type of interface units shall be assessed, in order to choose the most representative ones,
- identification of possible additional witness signals (cf. §13),
- identification of system components (processing units, communication units, networks) whose load shall be monitored during the avalanche (during phases 2 and 3 of the test),
- identification of potentially difficult points, which shall be subject to particular attention during the test preparation or execution.

6.5.2 Method

The system modeling shall observe the following steps:

- identification of the different paths taken by the avalanche, limited to those originating in the process, and terminating in the Level 2 system,
- identification of the technical functions used by these paths,
- breakdown of the different paths into technical functions,
- determination of the technical functions characteristics, as a function of the influencing parameters,

- consolidation of these characteristics for each path, as a function of the influencing parameters.

The system modeling will be concluded by the selection of the influencing parameters (and their set of values) subject to measure. The system modeling performed for the information transit times test may be used for this purpose, and completed.

6.5.3 Technical Functions

The main technical functions to be modeled are:

- A/D conversion,
- acquisition scanning,
- filtering,
- chattering processing,
- validity status management,
- grouping of variables for transmission,
- variables network transmission,
- minimum application processing.

6.5.4 Paths Breakdown

The paths taken by the avalanche shall be broken down into a succession of technical functions.

6.5.5 Technical Functions Characteristics

6.5.5.1 Technical Functions Characteristics

The technical functions shall be characterized by the elementary parameters used during the system modeling performed for the information transit times test (such as function activation mode, periodicity, duration, priority, interruptibility), and completed with:

- the buffers lengths,

- maximum flows,
- overflow management.

Networks will be handled as technical functions (transmission function).

The above elementary characteristics may vary with the system influencing parameters. They will be subject of a first consolidation, in order to establish for each technical function:

- a maximum instantaneous flow,
- an upstream buffer capacity,

which will generally be function and the system influencing parameters.

6.5.5.2 (System) Influencing Parameters

The system influencing parameters (or simply the influencing parameters) are the system parameters which are configurable for the purpose of a particular application, and which are likely to influence the system behavior during an avalanche. They are mainly:

- UT and UC cycle times,
- acquisition and emission rates,
- systematic processing parametering (dynamic filtering, static filtering, chattering processing, time tagging, ...),
- redundancy level of the different UT, UC, and networks,
- buffer lengths,
- size and complexity of the application program and database, represented in a simplified manner by an artificial static (i.e., excluding the load induced by the avalanche processing) processing unit load,
- type of interface units.

6.5.6 Conclusions of the System Modeling

The first result of the system modeling shall be to consolidate a maximum flow (as a function of influencing parameters) for each path taken by the avalanche, based on the

breakdown of these paths into technical functions and on the characteristics of these technical functions.

The second result shall be to precise, in view of the phases 2 and 3 of the test:

- the influencing parameters and conditions (and their set of values) subject to measure,
- the system components whose load shall be monitored during the avalanche.

6.5.6.1 Selection of Influencing Parameters

The influencing parameters which will be adjusted or modified to organize the different sets of measures, shall be selected based on the following criteria:

- system architecture and system configuration to be qualified or assessed,
- potential importance of the influence.

In absence of precise information on the system architecture or configuration, the most stringent values (but still realistic) will be chosen.

6.5.6.2 Selection of Component to be Monitored

The system components to be monitored (Processing units, communication units, or networks), i.e., whose load shall be measured continuously during and just after an avalanche, shall be selected based on the following criteria:

- possible requirements expressed in the requirements specification,
- existing technical facilities to measure these loads,
- resources and times constraints.

6.6 Influencing Conditions

The "system behavior during an avalanche" is an investigation group which is already based on an influencing conditions as defined in the IEC 1069 standard. The other influencing conditions likely to be considered during the present test (and only during the phase 2) are only those which are potentially correlated with the process avalanche, i.e.,:

- loss of power supply,

- load of the different (external) networks.

Other influencing conditions may be added, in case there are requirements which expressly combined them with process avalanche.

6.7 Documentation Required for the Test

The documents required in order to start the test program are the following:

- the present document,
- a document (e.g. Quality Plan) describing the Quality arrangements taken for the test, covering at least the following points:
  - responsibilities and competence of the persons in charge of test preparation and execution,
  - documentation management,
  - planning and progress control,
  - modification and configuration management (of the system under test and the test system),
- the supplier documentation, which shall:
  - correspond to the version of the system being tested,
  - enable a first system modeling,
- the architecture of the system to be assessed or qualified,
- the application structure (if available),
- the complete set of requirements likely to be verified by the "system behavior during an avalanche" test. These requirements shall include as a minimum a global (contractual or typical) avalanche profile, and possibly a controller avalanche profile.

6.8 Test Description

6.8.1 Test Organization

The issue is to generate events on the process inputs of the system, as per a given avalanche profile, and on a given system configuration, and to observe the behavior of the system.

The "system behavior during an avalanche" test is first broken down into three phases, as presented in Section 7, and corresponding to three different objectives.

Then each phase is broken down into several sub-tests, each sub-test corresponding to a given system configuration and a given avalanche profile.

Then each sub-test may be broken down into several measures, each measure corresponding to a given set of influencing parameters and conditions.

Each measure may be further broken down into several repetitions, each repetition being separated from the previous one by either a power supply interruption, or by a processing units re-initialization.

Suggested number of repetitions for each measure is 4, but this figure shall be confirmed in the test program. It may be:

- increased if the first repetitions indicate important performances standard deviations or unexplainable values,
- or decreased if the first repetition results match with the system modeling.

6.8.2 Configurations

6.8.2.1 System Under Test

Depending on the phase of the test, the configuration of the system under test shall contain:

- one (in phase 1) or two (in phase 2 and 3) programmable controllers, equipped each with:
  - 1 main rack, with its processing unit (UT1), and its two communication units (UC0 et UC1)

  - at minimum 2, and if possible the maximum number of extension racks foreseen in the future architecture, with their processing units (UT2), and their communication units (UC2)
  - its bus extension or intra-controller network
  - its power supply
- a set of interface units (UI), whose quantity will depend on the phase of the test (see description in Sections 6.8.3 thru 6.8.5),
- one maintenance/programming console, giving access to messages such as system errors messages or component load rates.

and for the phases 2 and 3 only:

- the inter-controller unit network, with the 2 controllers as its subscribers,
- the unit network with Level 2,
- the means to simulate the loads of the various networks, when these loads have been identified as possible influencing conditions.

The redundancy level of each component will be the one of the architecture to be qualified or assessed.

6.8.2.2 Test System

The test system configuration shall enable:

- the stimulation of all LOG and ANA inputs of the paths taken by the avalanche,
- the counting of the number of events occurring on the outputs of the paths taken by the avalanche,
- to monitoring of the witness signals.

For this purpose, one or more signal generators and a signal recorder shall be used.

6.8.2.2.1 Signal Generator(s)

The signal generator(s) shall be capable to perform the following functions:

- For the direct LOG inputs: generation of dynamic square signals, with a frequency covering the range 1 Hz to 1 kHz.
- For the direct ANA inputs: generation of voltage or current signals, covering the complete electrical range, and of various shapes (square, ramps, sinusoidal waveform) and covering the range 1 Hz to 1 kHz.
- For the network inputs: generation of change of states (for the LOG inputs) or variations (for the ANA inputs), with the maximum frequency allowed by the simulated network and system.
- For the all above inputs: capacity to count the number of cycles generated individually on each input.

6.8.2.2.2 Signal Recorder

The signal recorder shall be capable to:

- record the witness signals inputs and outputs (LOG and ANA, direct and network),
- compute the time elapsed between the event on the input, and the corresponding event on the output, with a precision equal or better than one millisecond, for all the witness signals,
- record the time tagged system error messages (if the system enables it),
- keep track (in writing as well as in a standard computer format) of the measures, in order to ensure the test traceability and reproducibility,
- count the number of events occurring at the inputs and outputs of the paths taken by the avalanche.

Some of these functions may be performed by a Level 2 system, or by using counters variables within the system under test.

6.8.3 Phase 1

6.8.3.1 Principle

This phase of the test first consists in the determination or approximation of the avalanche size above which the controller basic technical functions saturate, and then in the determination of the influencing parameters having an impact on this avalanche size. (See Section 6.5.5.2).

6.8.3.2 The Different Sub-Tests

The events will be generated on the process inputs of the system, in a progressive manner, and for each type of interface unit (UI) identified as significant during the system modeling:

- **sub-test 1**: triggering of a single input, with a single interface unit installed,
- **sub-test 2**: triggering of all the inputs of the interface unit, with only this interface unit installed,
- **sub-test 3**: triggering of a single input, with the maximum number of interface units installed in a single rack,
- **sub-test 4**: triggering of all the inputs of the interface unit, with the maximum number of interface units installed in a single rack,
- **sub-test 5**: triggering of a single input, with the maximum number of interface units in the maximum number of racks,
- **sub-test 6**: triggering of all the inputs of the interface unit, with the maximum number of interface units in the maximum number of racks,
- **sub-test 7**: triggering of all the inputs of the rack, with the maximum number of racks.

These sub-tests may be completed by intermediate sub-tests (such as triggering of a single input with the number of interface units just necessary to reach the system limits), in order to better approximate the avalanche threshold per type of basic technical function (channel acquisition, card acquisition and processing, rack acquisition and processing).

Based on the same principle, some of these sub-tests can be suppressed, if their objectives become irrelevant due to the system behavior.

The above sub-tests will be broken down into different measures, each measure corresponding to different influencing parameters (such as scanning frequency or priority), whose impact on the controller basic technical functions will have been demonstrated by the system modeling.

This breakdown of the sub-tests into several measures is limited to the first sub-tests. As soon as the importance of the influencing parameters as determined by the system modeling is confirmed by the first sub-test, only the most significant influencing parameters will be modulated, the other influencing parameters being kept equal to their most stringent values.

For each of the measures, the system will be loaded progressively, by increasing the input triggering frequency (f), in order to confine the avalanche threshold above which the controller basic technical functions (channel, card, and rack acquisition and processing) saturate within precise limits.

6.8.3.3 Configuration of the System Under Test

This phase of the test addresses only the system mechanisms, and not possible application processing in the processing units in the main racks (UT_1) and in the extension racks (UT_2). Therefore, no application will be loaded in these processing units, except those necessary to the witness signals (see Section 6.8.3.5).

This phase of the test does not address the inter controllers exchanges: the sub-tests will be carried out on a single controller.

The influencing conditions will not be adjusted: the sub-tests of this phase will be carried out on a controller in normal operation, without system failure, and without operator disturbances (either through Level 1, or through Level 2).

6.8.3.4 Avalanche Generation

The avalanche will be generated by injecting the following signals on the system :

The same signal, for all the LOG inputs chosen, having the following form:

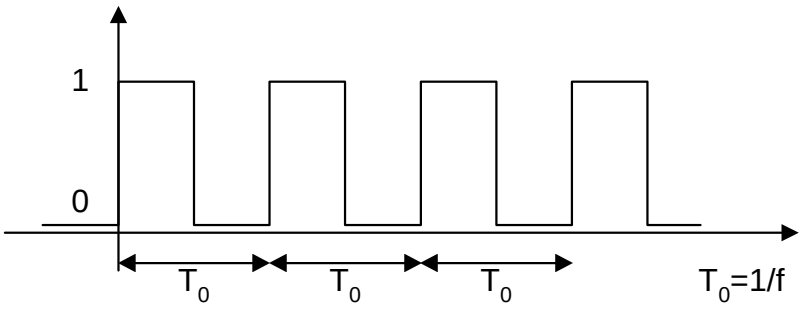


Figure B-8.

The same signal, for all the ANA inputs chosen, having the following form:

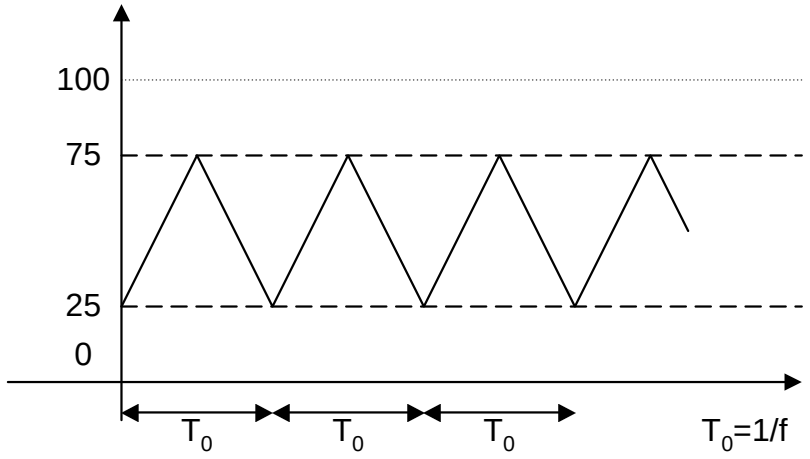


Figure B-9

For the ANA inputs, the variation will be between 25 et 75% of the electric range, in order not to take into account the possible high and low limits processing.

For the ANA inputs as well as for the LOG inputs, the triggering frequency will be increased by stage, as per the following curve:

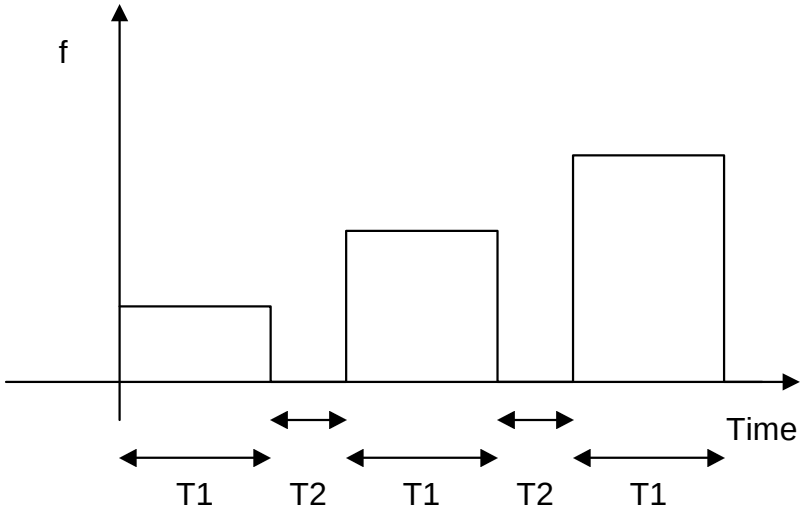


Figure B-10

where T1 = 2 minutes, and T2 is long enough to be sure that the previous avalanche has been completely processed by the system.

6.8.3.5 Witness Signals

The witness signals chosen to monitor the proper system operation during an avalanche are:

- a process output, defined as the recopy of a process input used also to stimulate the avalanche,
- a process output, defined as the recopy of a process input not part of a path taken by the avalanche,
- an output to Level 2, defined as the recopy of a process input used also to stimulate the avalanche,
- an output to Level 2, defined as the recopy of a process input not part of a path taken by the avalanche,

This list is not intended to be complete. Other witness signals may be used if shown necessary by the system modeling or the first sub-tests.

The witness inputs (those not part of a path taken by the avalanche) will be triggered at a frequency:

- low enough to ensure the correspondence between an event on the input, and the event on the output,
- high enough to allow an efficient monitoring of the witness signals.

6.8.3.6 Readings

During this phase, the controller behavior will be checked by the simultaneous monitoring of:

- the witness signals,
- possible messages on the front face of the different controller cards, or on the maintenance/programming console,
- the events counters facilities.

Each measure will be preceded by a reading of these witness signals (forms and response time) which will used as a reference for the different readings.

For each measure, the following readings shall be made:

- the triggering frequency at which the first disturbance on the system operation does appear,
- the time at which this disturbance appears (measured from the beginning of the avalanche)
- the disturbance characteristics:
  - indications on the front face of the controller cards, or messages on the maintenance/programming console,
  - response times deterioration,
  - witness signal output distortion,
  - Processing unit load (UT_1 or UT_2),
  - duration of the disturbance (if time limited),
  - whether it is systematic or not,
  - the number or proportion of events lost (i.e., not seen by the event counting facilities) on the outputs of the paths taken by the avalanche.

6.8.3.7 Results

The results expected from this first phase are:

- the maximum flows of each basic technical function:
  - acquisition and processing of a channel
  - acquisition and processing of a card
  - acquisition and processing of a rack
- the explanation of these limits, in relation with the results of the system modeling,
- the impact of the influencing parameters on these limits, in particular the importance of the interface units, in order to minimize the number of measures per sub-test in the next two phases.

6.8.4 Phase 2

6.8.4.1 Principle

This phase of the test consists in the generation of an avalanche with a given (contractual or typical) profile on the process inputs system, and the monitoring of the system behavior on the following aspects:

- proper execution and preservation of the performances of the missions selected during the requirements characterization (see Section 6.4.2.1),
- information made available by the system to the operator,
- system internal mechanisms behavior (processing units load, influence on the parts of the system not concerned by the avalanche, ...).

6.8.4.2 The Different Sub-Tests

In principle, this phase is made of as many sub-tests as there are couples (LOG + ANA) of contractual or typical avalanche profiles, i.e., normally only one.

However, in order to check the system behavior during the contractual or typical avalanche, without having to generate a potentially complex avalanche profile, it may be interesting to break down this phase into several sub-tests as follows:

- first sub-tests: utilization of a rectangular envelope avalanche profile whose duration is equal to the total duration of the contractual or typical avalanche, and whose constant event flow is equal to the maximum event flow of the contractual or typical avalanche.

In case the results of this sub-test are conclusive (i.e., if the system missions and performances comply with the expressed requirements), then phase 3 of the test can be carried out without further sub-tests for the phase 2. Otherwise, the phase 2 will be continued with:

- complementary sub-tests obtained by making progressively the avalanche profile more complex in order to approach the contractual or typical avalanche profile.

This or these sub-tests are broken down into several measures, by adjusting influencing parameters and conditions as determined during the system modeling.

6.8.4.3 Configuration of the System Under Test

The configuration of the system under test shall:

- enable the adjustments of the influencing parameters and conditions which have been selected during the system modeling,
- include the minimum application necessary to:
  - generate the output variables at the termination of the paths taken by the avalanche, and as per the ratio identified in Section 6.4.2.3.1,
  - cover a processing of each of the types of missions selected during the requirements characterization (see Section 6.4.2). These processings will be independent one from another, and will be performed on inputs not part of a path taken by the avalanche.

6.8.4.4 Witness Signals

The witness signals chosen to monitor the proper system operation during the typical or contractual avalanche are those corresponding to the systems missions identified during the requirements characterization (see Section 6.4.2):

- process LOG input and simple transfer to a LOG output toward Level 2,
- process ANA input and simple transfer to an ANA output toward Level 2,
- process LOG input and transfer to a LOG output toward Level 2 (automatic logic control),
- process ANA input and transfer to an ANA output toward Level 2 (through a PID modulating loop),
- LOG command from Level 2 and simple transfer to a LOG output toward the process,
- ANA command from Level 2 and simple transfer to a ANA output toward the process,
- LOG command from Level 1 HMI and simple transfer to a LOG output toward the process,
- ANA command from Level 1 HMI and simple transfer to a ANA output toward the process.

If time tagging function is one of the mission to be monitored, then the first two signals shall be duplicated.

The witness signals inputs will be triggered at a frequency:

- low enough to ensure the correspondence between an event on the input, and the event on the output,
- high enough to allow an efficient monitoring of the witness signals.

6.8.4.5 Readings

During this phase, the controller operation and performances will be checked by the simultaneous monitoring (during the complete duration of the avalanche, as well as during a period of time necessary to make sure that the avalanche has been fully absorbed by the system), of:

- the inputs and outputs of the witness signals,
- the messages intended for the (control or maintenance) operators:
  - on the front faces of the controller cards, or
  - on the programming/maintenance console, or
  - sent to the Level 2 system,
- the load of different processing and communication units, or networks, as identified during the system modeling,
- the event counting facility.

Each measure will be preceded by a reading of these witness signals (forms and response time) which will used as a reference for the different readings.

For each measure, the following readings shall be made:

- apparition or not of a disturbance,
- the time at which this disturbance appears (measured from the beginning of the avalanche),
- the disturbance characteristics:

- indications on the front face of the controller cards, or messages on the maintenance/programming console,
- response times deterioration,
- witness signal output distortion,
- processing or communication unit load, or network load,
- duration of the disturbance (if time limited),
- whether it is systematic or not,
- the number or proportion of events lost (i.e., not seen by the event counting facilities) on the outputs of the paths taken by the avalanche.

6.8.4.6 Results

The results expected from this second phase are for each sub-test:

- proper execution or not of the chosen missions (those corresponding to the selected witness signals),
- maximum deterioration values for the selected performances (response time and accuracy) of the same chosen missions,
- type and quality of the information made available to the operator,
- maximum load of the components (processing units, communication units, networks) during the 'avalanche,
- avalanche absorption time, defined as the duration between:
  - the end of the avalanche generation,
  - the moment the main component loads are back to their normal reference loads (i.e., their loads measured in the absence of avalanche),
- impact of the influencing parameters and conditions on all previous characteristics.

6.8.5 Phase 3

6.8.5.1 Principle

This last phase of the test consists in the determination of the boundary avalanche, i.e., the avalanche above which the system does not fulfill its missions. This boundary avalanche is obtained by progressively:

- increasing the typical or contractual avalanche profile (in case the phase 2 of the test was carried out),
- or decreasing the basic technical functions limits obtained during phase 1 (in case the phase 2 was not carried out).

In both cases, the influencing parameters and conditions are fixed.

6.8.5.2 The Different Sub-Tests

The different sub-tests of this phase are obtained by the progressive modification of the avalanche profile, starting from the following profile:

- [1] After a phase 2: the contractual or typical avalanche profile, or if the first sub-test results were conclusive (see Section 6.8.4.2), the rectangular envelope avalanche profile.
- [2] In the absence of phase 2, i.e., when a controller avalanche profile cannot be supplied: the combination of two (1 LOG + 1 ANA) rectangular profiles obtained using the limit values of the controller basic technical functions capacities.

Then the next sub-tests are obtained by increasing (case [1]) or decreasing (case [2]) of these avalanche profiles by steps of 10 % of the flows of events (LOG and ANA simultaneously), without modification of the avalanche duration.

The phase will end with the first sub-test where the first loss of missions occurs (case [1]) or where all missions are restored (case [2]), as defined precisely beforehand (see Section 6.4.2.1).

Each sub-test consists of a single measure, knowing that:

- the influencing conditions are not taken into account during this phase of the test (no loss of power supply, and networks loads fixed at their most stringent but realistic values),
- the influencing parameters are fixed at their most stringent but realistic values.

Only the last sub-test may be broken down into several measures, in order to check the importance of the influencing parameters when the avalanche generated is close to the maximum manageable by the system.

6.8.5.3 Configuration of the System Under Test

The configuration of the system under test used during this phase will be the same as the one used during the phase 2.

6.8.5.4 Witness Signals

The witness signals used during this phase will be the same as the ones used during the phase 2.

6.8.5.5 Readings

The reading s made during this phase will be the same as the ones made during the phase 2.

6.8.5.6 Results

The results expected from this third phase are:

- a boundary rectangular avalanche profile (combination of a LOG and an ANA profile), for which:
  - when the system is subject to an avalanche with this profile, there is no loss of system missions,
  - but when the system is subject to an avalanche with the same profile increased by 10% (in the flow of LOG and ANA events), at least one mission is lost,
- the importance of the influencing parameters for this avalanche profile,
- the avalanche absorption time of this boundary avalanche.

6.9 Expected Results

The results expected from this test are of various natures, depending on the objectives this test fulfills:

- To understand and master the system, the test should insure:
  - the validation of the system modeling,
  - the validation of the system supplier data,
  - the detection of possible system operation anomalies.
- To guide the system realization, the test should supply:
  - recommendations for the architecture design,
  - recommendations for the system configuration, specially for the influencing parameters values.
- To continue the system qualification (when applicable), the test should supply:
  - recommendations for possible additional analysis or simulation required to complete the (Level 1) control system evaluation,
  - recommendations for possible additional analysis or simulation required to complete the overall control system or the other systems evaluation,
  - a list of additional information required from the supplier.
- To formally demonstrate the fulfillment of the requirements related to the system behavior during an avalanche (as long as the recommendations given on the system architecture or configuration are followed), the test should confirm:
  - the maximum performances deterioration occurring during an avalanche,
  - the avalanche absorption times,
  - the main influencing parameters and conditions, and their impact on the system behavior.

7 Time Tagging

7.1 How to Use this Document in the Different Steps of the Test Preparation and Execution

The different steps of the evaluation process, leading to the writing of the test program and to the test execution are summarized in Figure B-11. The present document gives principles and recommendations for these various steps:

- Definition of the system under evaluation (to be assessed or qualified), of its architecture, of its interfaces, and comparison with the envelope architecture proposed in Section 4,
- Characterization of the requirements (Section 7.3.2), starting from the requirements identified beforehand (Section 7.3.1),
- Selection of the different paths and pair of paths to be tested (Section 7.3.3),
- System modeling (Section 7.4),
- Selection of the influencing parameters to be examined (Section 7.4.4),
- Selection of the influencing conditions to be examined (Section 7.5),
- Breakdown of the test into sub-tests and measures (Section 7.7.1),
- Definition of the system under test and of the test system configurations (Section 7.7.2),
- Sub-tests execution and readings (Sections 7.7.3 and 7.7.4),
- Test results analysis and comparison with the system modeling results (Section 7.7.5).

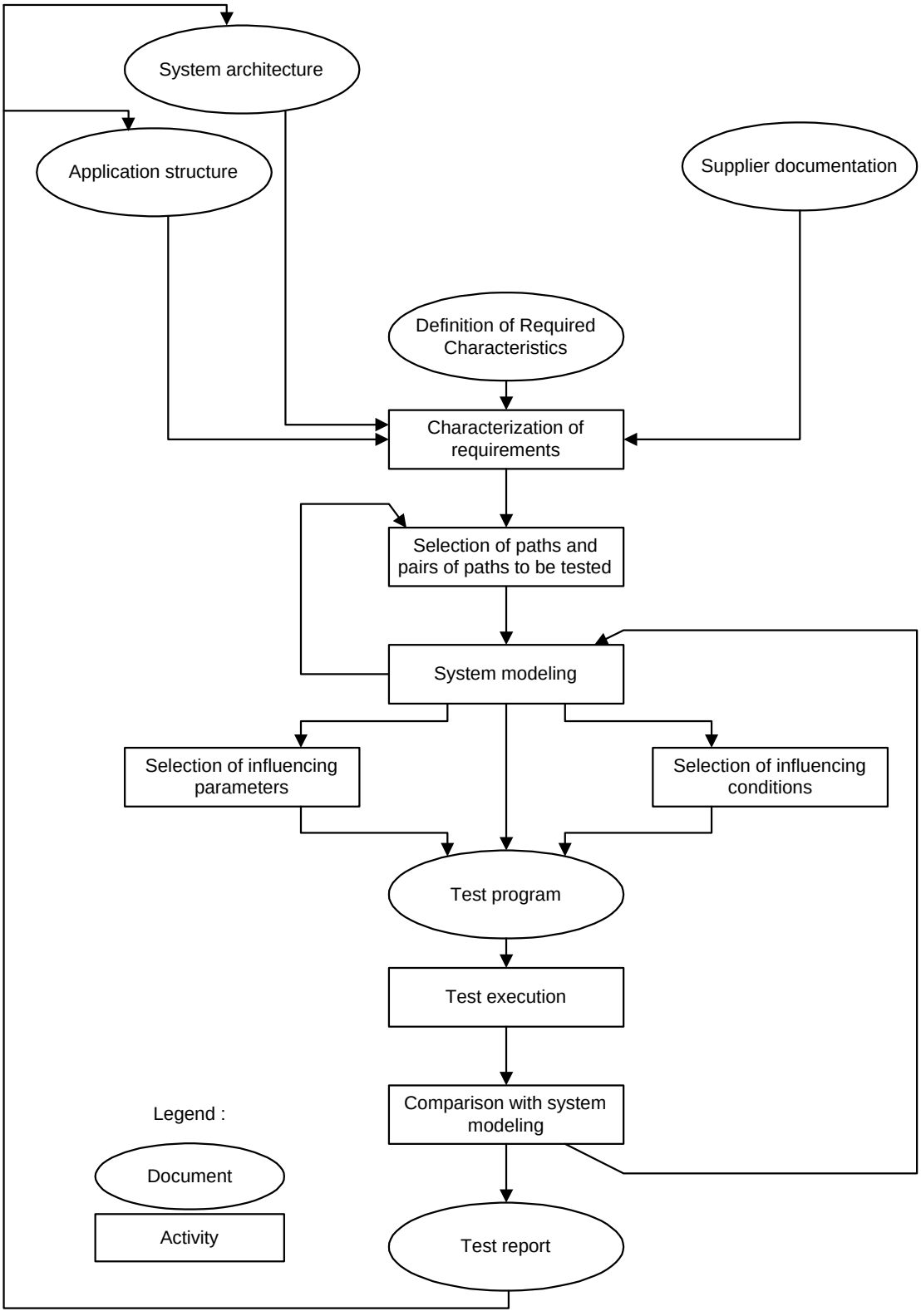


Figure B-11. "Time Tagging" Test Preparation and Execution Process

7.2 Test Objectives

The purpose of this test is to evaluate globally and in detail the principles and the quality of the time tagging function of all acquired or calculated variables which are time tagged by the system.

Those variables which are likely to be time tagged are:

- the inputs acquired by the system from the process or from other systems,
- the operator orders received from Level 2 system, or from Level 1 Human Machine Interface (such as maintenance console or individual command/setpoint station),
- the variables computed by the system, using acquired or diagnostic variables.

These time tagged variables are then (cyclically or event-driven) transmitted by the system to other systems (Level 2 system, Level 1 HMI, or other systems) accompanied (individually or in group) by a date (i.e., date, hour, second, and millisecond).

N.B.: In the rest of this document, the word "date" means date with hour and second, and when applicable, millisecond.

The first objective is to explain the acquired or calculated information time tagging characteristics, based on the following mechanism:

- acquisition of an external reference date,
- possible sync. pulse acquisition,
- date distribution within the system,
- system components synchronization,
- events time tagging,
- transmission of time tagged events.

The second objective is to compare the results obtained by a system modeling, with the results obtained by the test.

These time tagging characteristics can be sorted by degrees of increasing difficulty[2]:

[2] Ref. glossary (Section 3) and typical architecture (Section 4) for the definitions of the different system components.

- time tagging relative accuracy between two acquisition performed on the same interface unit (UI),
- time tagging relative accuracy between two acquisitions or computations performed on the same rack,
- time tagging relative accuracy between two acquisitions or computations performed on the same controller,
- time tagging relative accuracy between two acquisitions or computations performed on the two different controllers,
- time tagging absolute accuracy of an acquisition or computation (= time tagging relative accuracy between this accuracy or computation, and an external reference clock).

The third objective is to measure the importance of impact of the influencing parameters and conditions on these time tagging characteristics, as well as to assess the behavior of the system when the date is changed.

In case of a system qualification, the test shall lead to the formal demonstration that the requirements expressed in the requirements specification and related to the time tagging characteristics are met.

In case of a system assessment, the test shall verify that the system time tagging characteristics are compatible with the standard requirements for nuclear power plants control systems.

Finally, the test shall supply technical information which is reliable, repeatable, and traceable, and which will:

- enable the pursuit of the system evaluation process, based on the level of confidence acquired,
- provide guidance on how to structure the future application programs,
- provide guidance on how to build the control system architecture,
- feed the next phases of the control system qualification process.

7.3 Requirements

7.3.1 Typical Requirements on Service Functions

The present chapter proposes a set of typical requirements which can be verified directly or indirectly by the "time tagging" test. It is a guide for the preparation of the test. The person in charge of the preparation of the test will make sure, by reading thoroughly the requirements specification, that all related requirements have been identified.

In the case of the REP 2000 qualification process, this action is normally performed during the establishment of the referential of characteristics.

In the case of a system assessment, the reading of this chapter may help the person in charge of the preparation of the test to better identify the purpose of the test, and therefore help him to properly structure the test.

These typical requirements apply on the following characteristics:

- **Type of time tagged information**, such as:
  - threshold overshoot,
  - variable off limits,
  - inhibition, replacement.
- **Time tagging absolute accuracy**, on variable such as:
  - LOG input, on a dedicated (e.g., SoE) card,
  - LOG input, on a standard input card,
  - ANA input, on a dedicated card,
  - ANA input, on a standard input card,
  - system maintenance variable,
  - computed variable,
  - alarm variable,
  - LOG control,

  - ANA control.

- **Time tagging absolute accuracy**, between two variables such as:
  - any two LOG inputs,
  - two LOG inputs arranged optimally,
  - any two ANA inputs,
  - two ANA inputs arranged optimally.
- **Non influence on the time tagging accuracy**, of points such as:
  - number of channels used on the interface unit,
  - position of the channel on the interface unit,
  - the type of transition (up or down) of the event,
  - switch over in case of redundant component,
  - load of system components.
- **Behavior on the loss of the reference clock**
  - maximum allowed drift,
  - operator information.
- **Behavior on loss and reinsertion of a component**
  - resynchronization duration.
- **Behavior on (automatic/manual) change of date and time**
  - daylight saving time,
  - Year 2000.

7.3.2 Characterization of Requirements

The requirements likely to be verified by the "time tagging" test, as identified in the previous chapter, need to be characterized, i.e., translated in terms of time tagging absolute (resp. relative) accuracy for a given path (resp. for a given pair of path).

This chapter defines precisely the studied characteristics (time tagging accuracy), and then identify the different paths within the system, which are characterized by the time tagging accuracy.

7.3.2.1 Preliminary Definitions

Path

The time tagging accuracy is concerned with the system outputs which are accompanied by a date. Each output variable can be considered as the output of a "path" representing the route taken by the signal, each path being defined by:

- its input (in the case of self diagnostic variables, the path input is internal to the system) and its output at the borders of the system,
- the physical trajectory taken by the signal (type of input card; set of processing units, communication unit, and networks used; type of output card), and
- the type of processing performed on this signal (systematic or application).

The output variables computed using several system inputs are the outputs of several paths. However, **this document does not address the time tagging accuracy related to two events occurring quasi simultaneously on two inputs of a computed variable**. The validity of this hypothesis will be checked during the system modeling. In case this hypothesis appears too restrictive, then the influence of two (or more) quasi simultaneous events on the time tagging characteristics will be studied, by adding the variation of another input of a given computed variable as an influencing condition.

Event

An event, associated to an (input, output, or internal) variable, is defined as follows:

- for a LOG variable: an event is a change of state (0 → 1 or 1 → 0)
- for an ANA variable: an event is a significant variation of this variable, i.e., higher than a predefined percentage of the range of this variable.

For the purpose of this test, an event on an input shall always be considered as instantaneous, i.e., of a duration which is negligible compared to the studied characteristics.

Time tagging accuracy

Two types of time tagging accuracy can be defined: time tagging absolute accuracy and time tagging relative accuracy.

The **time tagging absolute accuracy** is the maximum difference between:

- the date accompanying an event on a system output, whether this output is updated cyclically or event-driven, and
- the date at which the associated event occurred on the input of the path, and measured with the time of the external reference clock.

This characteristics is therefore associated to a given path.

The time tagging relative accuracy between two time tagged system outputs is:

- either the maximum difference between the dates of two events on these two time tagged outputs, these two events being the consequences of two exactly simultaneous events on the inputs of the paths,
- or, in an equivalent definition, the minimum duration between any two events on the system inputs, below which the corresponding events on the outputs of the system cannot be discriminated in time any more.

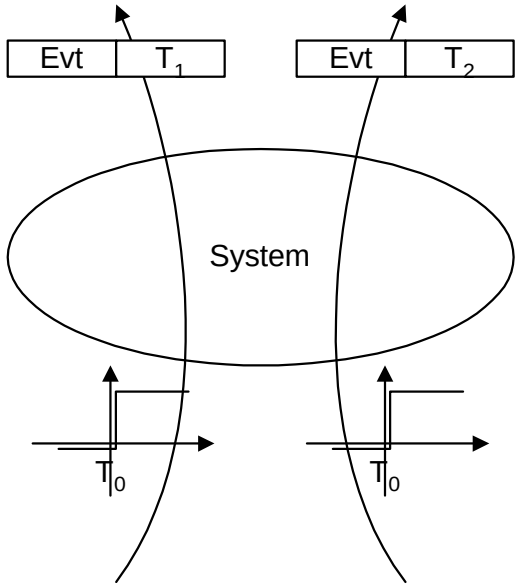
This characteristics is therefore associated to a given pair of paths.

Note 1: the time tagging absolute accuracy is meaningless when the system is not synchronized by an external reference clock.

Note 2: the transmission mechanisms (cyclically or event driven) of the outputs to the other systems is transparent for what follows.

Note 3: this document does not address the case where the variables received are already time tagged, except when they are "retagged" by the system.

The figure below summarizes the above definitions:



T_0 measured using the external clock reference time

Time tagging absolute accuracy: $|T_1-T_0|$

Time tagging relative accuracy: $|T_2-T_1|$

Figure B-12

From these definitions:

- It is possible to conclude that the time tagging relative accuracy is better than twice the time tagging absolute accuracy.
- It is not possible to conclude on the time tagging absolute accuracy based on the sole knowledge of the time tagging relative accuracy.

7.3.2.2 The Paths

7.3.2.2.1 The System Inputs and Outputs

Systems Connected	I_{LOG}	I_{ANA}	O_{LOG}	O_{ANA}
Level 2 system (N)	N1	N3	N2	N4
Level 1 HMI (C)	C1	C3	C2	C4
Other systems (through unit networks) (E)	E1	E3	E2	E4
Process, conventional control means, other controllers or other systems (P, O, A, or S)	X1	X3	Not applicable (to be verified for fieldbus outputs)	
Inputs internal to the system (e.g., self diagnostics variables)	I1	I3	Not applicable	

7.3.2.2.2 Physical Trajectories

Based on the envelope architecture identified in the previous chapter, there are many possible physical trajectories, which can be structured around all the possible combinations of I/Os types.

- [X→N] From a conventional control means, the process, other systems, or other controllers and toward a Level 2 system, the different trajectories are obtained by selecting:
  - whether the interface unit is on the main rack or on an extension rack
  - the type of the interface unit
- [X→E] From a conventional control means, the process, other systems, or other controllers and toward other systems, the different trajectories are obtained by selecting:
  - whether the interface unit is on the main rack or on an extension rack
  - whether the controller containing the unit interface is directly connected to the other system or not
  - the type of the interface unit
- [X→C] From a conventional control means, the process, other systems, or other controllers, and toward a Level 1 HMI, the different trajectories are obtained by selecting:
  - whether the interface unit is on the main rack or on an extension rack
  - whether the input and the output belong to the same controller or not
  - the type of the interface unit
- [I→N] From an internal diagnostic variable and toward a Level 2 system, there is only one possible trajectory.
- [I→E] From an internal diagnostic variable and toward other system, the different trajectories are obtained by selecting:
  - the controller generating the diagnostic variable is directly connected to the other system, or not

- [I→C] From an internal diagnostic variable and toward a Level 1 HMI, the different trajectories are obtained by selecting:

  — the controller generating the diagnostic variable is directly connected to the Level 1 HMI, or not

- [N↔N] Between two Level 2 systems, the different trajectories are obtained by selecting:

  — whether the two Level 2 systems are distinct or not

- [E↔N] Between a Level 2 system, and another system, the different trajectories are obtained by selecting:

  — whether the Level 2 system and the other system belongs to the same network or not

- [C↔N] Between a Level 2 system and a Level 1 HMI, there is only one possible trajectory.

- [E↔E] Between 2 other systems, the different trajectories are obtained by selecting:

  — whether these other systems are distinct and belong to different network, are distinct and belongs to the same network, or are not distinct

- [C↔E] Between a Level 1 HMI and another system, the different trajectories are obtained by selecting:

  — whether the controller to which the Level 1 HMI is connected, is directly connected to the other system or not

- [C↔C] Between two Level 1 HMI, the different trajectories are obtained by selecting:

  — whether the two Level 1 HMI are distinct and connected to two different controllers, are distinct and connected to the same controller, or are not distinct

7.3.2.2.3 Processing

Processing performed on a signal can be divided into two categories, the systematic processing and the application processing:

- systematic processing is the system or pre-programmed (configurable or not) processing which is potentially performed on all variables of the same kind (A/D conversion, filtering, chattering processing, ...),

- application processing is the programmed processing, adapted per variable.

Systematic processing to be tested can be:

- standard systematic processing performed for each type of variable,
- self diagnostic,
- off limits,
- inhibition,
- replacement.

Application processing to be tested can be:

- a minimum logic processing,
- a minimum analogue processing,
- a minimum mixed processing enabling the conversion of an ANA input into an LOG output and vice versa.

The application processing will be chosen as simple as possible, but still representative of the time tagging mechanisms for computed variables.

As a general rule:

- the minimum logic or analogue processing will be: Output = Input.
- the mixed processing will be:
  - f(ANA) = 0 if ANA < threshold and f(ANA) = 1 if ANA > threshold (without dead band)
  - g(TOR) = ANA1 if TOR = 0 et g(TOR) = ANA2 if TOR = 1

The application processing selected may be reviewed after the system modeling step, if it appears that:

- some application processing use specific components or operation modes (e.g., special modules),
- or the minimum application processing selected is not representative of the normal time tagging mechanisms, due to its simplicity.

7.3.3 Selection of the Paths and Pairs of Paths to be Tested

As indicated in Section 7.3.2, the time tagging accuracy characterizes:

- the different paths for the time tagging absolute accuracy,
- the different pairs of paths for the time tagging relative accuracy.

In view of the potential number of paths, and all the more the number of pairs of paths, it is absolutely compulsory to select the paths which will be subject to test. This selection will be made on the basis of the following criteria:

- the requirements expressed in the requirements specification (if any),
- how the time tagged information is used by the other systems,
- the time and resources constraints,
- the foreseen system architecture and application structure to be assessed or qualified,
- data available through other analysis and tests means (e.g., return of experience, supplier's data, ...),
- the possibility to generate events on the system inputs synchronously with the external reference clock,
- the two pre-selections proposed hereafter.

This selection may be revised or improved when the results of the system modeling or of the first sub-tests are available, particularly:

- the system modeling enables a better understanding of the time tagging mechanisms, and therefore a reduction in the number of representative paths,
- conclusive tests obtained on the time tagging absolute accuracy enable a reduction in the number of measures on the time tagging relative accuracy characteristics.

For the time tagging absolute accuracy characteristics, the following pre-selection of paths is proposed:

Path	**Description**			
Designation	**Input**	**Trajectory**	**Processing**	**Output**

Standard LOG input sent to Level 2 (without application processing)	X1	LOG input on extension rack, standard UI	Standard systematic processing, no application processing	N2
Dedicated LOG input sent to Level 2 (without application processing)	X1	LOG input on extension rack, dedicated UI (SoE)	Standard systematic processing, no application processing	N2
Standard LOG input sent to Level 2 (with minimum application processing)	X1	LOG input on extension rack, standard UI	Standard systematic processing, minimum logic application processing	N2
Standard ANA input sent to Level 2 (without application processing)	X3	ANA input on extension rack, standard UI	Standard systematic processing, no application processing	N4
Dedicated ANA input sent to Level 2 (without application processing)	X3	ANA input on extension rack, dedicated UI	Standard systematic processing, no application processing	N4
Standard ANA input sent to Level 2 (with minimum application processing)	X3	ANA input on extension rack, standard UI	Standard systematic processing, minimum analogue application processing	N4
Threshold monitoring on ANA input, to Level 2 system	X3	ANA input on extension rack, standard UI	Standard systematic processing, mixed application processing (threshold monitoring)	N2

These paths may possibly be duplicated with outputs toward Level 1 HMI, if the system modeling establishes that the time tagging mechanisms are different.

For the time tagging relative accuracy characteristics, the following pre-selection of pairs of paths is proposed:

Pairs of paths	**Description**		
Designation	**Path 1**	**Path 2**	**Relation b/w the**

			paths
2 standard LOG inputs on the same UI (without application processing)	Standard LOG input sent to Level 2 (without application processing)	Standard LOG input sent to Level 2 (without application processing)	The two inputs are on the same UI
2 standard LOG inputs on the same rack (without application processing)	Standard LOG input sent to Level 2 (without application processing)	Standard LOG input sent to Level 2 (without application processing)	The two inputs are on the same rack, but on 2 different UI
2 standard LOG inputs on the same controller (without application processing)	Standard LOG input sent to Level 2 (without application processing)	Standard LOG input sent to Level 2 (without application processing)	The two inputs are on the same controller, but on two different racks
2 standard LOG inputs on two different controllers (without application processing)	Standard LOG input sent to Level 2 (without application processing)	Standard LOG input sent to Level 2 (without application processing)	The two inputs are on two different controllers
2 standard LOG inputs on the same UI (with minimum application processing)	Standard LOG input sent to Level 2 (with minimum application processing)	Standard LOG input sent to Level 2 (with minimum application processing)	The two inputs are on the same UI
2 standard LOG inputs on the same rack (with minimum application processing)	Standard LOG input sent to Level 2 (with minimum application processing)	Standard LOG input sent to Level 2 (with minimum application processing)	The two inputs are on the same rack, but on 2 different UI
2 standard LOG inputs on the same controller (with minimum application processing)	Standard LOG input sent to Level 2 (with minimum application processing)	Standard LOG input sent to Level 2 (with minimum application processing)	The two inputs are on the same controller, but on two different racks
2 standard LOG inputs on two different controllers (with minimum application processing)	Standard LOG input sent to Level 2 (with minimum application processing)	Standard LOG input sent to Level 2 (with minimum application processing)	The two inputs are on two different controllers

Pairs of paths	**Description**		
Designation	**Path 1**	**Path 2**	**Relation b/w the paths**
2 standard ANA inputs on the same UI (without application processing)	Standard ANA input sent to Level 2 (without application processing)	Standard ANA input sent to Level 2 (without application processing)	The two inputs are on the same UI
2 standard ANA inputs on the same rack (without application processing)	Standard ANA input sent to Level 2 (without application processing)	Standard ANA input sent to Level 2 (without application processing)	The two inputs are on the same rack, but on 2 different UI
2 standard ANA inputs on the same controller (without application processing)	Standard ANA input sent to Level 2 (without application processing)	Standard ANA input sent to Level 2 (without application processing)	The two inputs are on the same controller, but on two different racks
2 standard ANA inputs on two different controllers (without application processing)	Standard ANA input sent to Level 2 (without application processing)	Standard ANA input sent to Level 2 (without application processing)	The two inputs are on two different controllers
2 standard ANA inputs on the same UI (with minimum application processing)	Standard ANA input sent to Level 2 (with minimum application processing)	Standard ANA input sent to Level 2 (with minimum application processing)	The two inputs are on the same UI
2 standard ANA inputs on the same rack (with minimum application processing)	Standard ANA input sent to Level 2 (with minimum application processing)	Standard ANA input sent to Level 2 (with minimum application processing)	The two inputs are on the same rack, but on 2 different UI
2 standard ANA inputs on the same controller (with minimum application processing)	Standard ANA input sent to Level 2 (with minimum application processing)	Standard ANA input sent to Level 2 (with minimum application processing)	The two inputs are on the same controller, but on two different racks
2 standard ANA inputs on two different controllers (with minimum application processing)	Standard ANA input sent to Level 2 (with minimum application processing)	Standard ANA input sent to Level 2 (with minimum application processing)	The two inputs are on two different controllers

7.4 System Modeling

7.4.1 Objectives

The objectives of the system modeling are:

- identification of the influencing parameters whose impact on the time tagging accuracy will be measured,
- computation of theoretical time tagging absolute and relative accuracy (for the paths and pairs of paths selected beforehand), as a function of these influencing parameters, for future comparison with the results of the time tagging accuracy measures,
- confirmation of the paths and pairs of paths to be selected for the test,
- identification of potentially difficult points, which shall be subject to particular attention during the test preparation or execution.

7.4.2 Method

The system modeling shall observe the following steps:

- identification of the time tagging components, i.e., those which associate a date to the events on acquired or computed variables,
- identification of the date distribution mechanisms, as well as the possible sync pulses distribution mechanisms within the system, from the external reference clock, up to the time tagging components synchronization,
- computation of the absolute accuracy of the date available within the time tagging components (i.e., the maximum difference with the reference date),
- computation of the maximum difference between two dates available within two different time tagging components at the same moment,
- analysis of the consequences of a change of date, or a loss of the distribution of date messages or sync pulses,
- identification of the minimum and maximum transit times between the occurrence of an event on a system input (on the selected paths), and the detection of this event by the relevant time tagging component,

- analysis of the time tagging mechanisms in the time tagging components, specially on:

  — the possible taking into account of the above minimum transit times by the time tagging component,

  — the date format accuracy,

- identification and computation of possible time tagging accuracy deterioration (along the selected paths) after the time tagging itself.

The system modeling is concluded with the computation of two types of characteristics:

- the time tagging absolute accuracy for each of the selected paths (cf. §8.3), obtained as the sum of:

  — the maximum transit time between the occurrence of an event on the path input, and its detection by the relevant time tagging component, possibly reduced if such transit times is taken into account by the time tagging component,

  — the absolute accuracy of the date available within the time tagging component,

  — and the intrinsic accuracy of the time tagging mechanism.

- the time tagging relative accuracy for each of the selected pair of paths (cf. §8.3), obtained as the sum of:

  — the greatest possible difference between two transit times (one for each of the paths), measured between the occurrence of an event on a path input, and its detection by the relevant time tagging component,

  — maximum desynchronizing between the two time tagging components (if the two paths used different time tagging component),

  — and the intrinsic accuracy of the time tagging mechanism (if the two paths use the same time tagging component), or the sum of the two intrinsic accuracies (if the two paths use different time tagging mechanisms).

7.4.3 Transit Time Up To The Time Tagging Components

In order to compute the (maximum and minimum) transit times on the part (i.e., from the path input, up to the relevant time tagging component) of all the selected paths, the results obtained by the system modeling achieved for and validated by the "information transit times" test should be used.

These transit times will generally depend on some influencing parameters (as defined in the next paragraph).

7.4.4 (System) Influencing Parameters

The system influencing parameters (or simply the influencing parameters) are the system parameters which are configurable for the purpose of a particular application, and which are likely to influence the time tagging characteristics of the system. They are mainly:

- UT and UC cycle times,
- acquisition rates,
- systematic processing parametering (dynamic filtering, static filtering, chattering processing),
- redundancy level of the different UT, UC, and networks,
- size and complexity of the application program and database, represented in a simplified manner by an artificial UT load,
- position of the input on the interface unit,
- number of inputs used per interface unit,
- number of interface units per rack,
- number of racks and interface units per controller,
- number of controllers, racks and interface units per system,

The influencing parameters which will be adjusted or modified to organize the different sets of measures, shall be selected based on the following criteria:

- system architecture and system configuration to be qualified or assessed,
- potential importance of the influence,
- time and resources constraints.

7.5 Influencing Conditions

Among all possible influencing conditions as identified in the [1069] standard, those likely to have an actual impact on the time tagging accuracy are the following:

- system tasks: on-line application modification, operation in degraded mode, on-line module insertion,
- personal: access to the system using the Level 1 HMI,
- process: I/Os flow variation,
- utilities: disturbances on the power supply,
- environment: electromagnetic disturbances,
- available services: without influence,
- other systems linked to the system: network load (with Level 2, with other systems), external reference clock.

The influencing conditions such as "I/Os flow variation" are handled in the "System behavior during an avalanche" investigation group, and not in the "Time tagging" investigation group.

The influencing conditions such as "utilities" and "environment" are handled in the "Environment" investigation group, and not in the "Time tagging" investigation group.

Therefore, the influencing conditions which will be examined during the present time tagging test are of two types:

- influencing conditions for which several values or configurations will be subject to different measures (with the definition of measure as given in Section 3):
  - load of the different networks,
  - system operation with the loss of an UT, an UC, an UI, a network or a fieldbus (if the system configuration enables such an operation).
- influencing conditions for which a measure (with the definition of measure as given in Section 3) will be carried out by generating one of the following events:
  - module (UT, UC, UI) on-line extraction and reinsertion ,
  - on-line system application modification and loading,

— operator intervention on the maintenance/programming console,

— loss of the external reference clock,

— automatic (by the external clock) or manual (by the operator) change of date.

The selection of these different influencing conditions which will be examined will be based on the following criteria:

- requirements expressed in the requirements specification (if any),
- time and resources constraints,
- data available through other analysis and tests means (e.g., return of experience, supplier's data),
- results of the system modeling.

As a minimum, the loss of the external reference clock, and the change of date will be retained.

7.6 Documentation Required for the Test

The documents required in order to start the test program are the following:

- the present document,
- a document (e.g., Quality Plan) describing the Quality arrangements taken for the test, covering at least the following points:

  — responsibilities and competence of the persons in charge of test preparation and execution,

  — documentation management,

  — planning and progress control,

  — modification and configuration management (of the system under test and the test system),

- the supplier documentation, which shall:

  — correspond to the version of the system being tested

  — enable a first system modeling

- the architecture of the system to be assessed or qualified,
- the application structure (if available),
- the complete set of requirements likely to be directly or indirectly verified by the time tagging test. These requirements:
  - may be either directly available in the form of a referential of characteristics, containing the sub-set of requirements which need to be verified during the time tagging test in the evaluation phase of the support system,
  - or may need an extraction from a document specifying generic requirements.

7.7 Test Description

7.7.1 Test Organization

The issue is to measure time tagging absolute (resp. relative) accuracy on the different selected paths (resp. pairs of paths) selected beforehand (as described in Section 7.3.3), and with varying selected influencing parameters and conditions (Sections 7.4.4 and 7.5).

The sub-tests

The time tagging test is first broken down into several sub-tests, each sub-test corresponding to a given pre-selected path or pair of paths. The first sub-tests will address the time tagging absolute accuracy, the last ones will address the time tagging relative accuracy.

The measures

Then each sub-test may be broken down into several measures, each measure corresponding to a given set of influencing parameters and conditions. The influencing parameters and conditions to be examined are selected during the system modeling phase.

The influencing conditions which are modified by the generation of particular events, such as the loss of the external reference clock, or a change of date, will preferably be examined in the time tagging absolute accuracy sub-tests, and only on the most characteristic paths.

The other influencing conditions, which are modified by adjusting values or configurations, as well as the influencing parameters, may be examined on a limited number of sub-tests. Once the importance of such influencing conditions or parameters

is confirmed by the first sub-tests, these influencing conditions and parameters will be frozen with their most stringent values for the other sub-tests.

Repetitions

Each measure may be further broken down into several repetitions, each repetition being separated from the previous one by either a power supply interruption, or by a processing units re-initialization.

Suggested number of repetitions for each measure is 4, but this figure shall be confirmed in the test program. It may be:

- increased if the first repetitions indicate an time tagging accuracy standard deviation or unexplainable values,
- or decreased if the first repetition results match with the system modeling.

7.7.2 Configurations

7.7.2.1 System Under Test

Configuration of the system under test shall be such as to enable to test all the selected paths and pair of paths. The preferred pairs of paths, as identified in §8.3, lead to the definition of the following minimal configuration:

- Two programmable controllers, equipped each with:
  - 1 main rack, with its processing unit (UT_1), and its two communication units (UC_0 et UC_1)
  - 1 extension rack, with its processing unit (UT_2), and its communication unit (UC_2)
  - its bus extension or intra-controller network
  - its power supply
- a set of interface units (UI), containing two UI of each type, and in sufficient quantity to ensure that the influencing parameters (such as number of cards per rack) as defined during the system modeling are properly represented,
- one maintenance/programming console,
- the Level 1 HMI, if any,

- the inter-controller unit network, with the 2 controllers as its subscribers,
- the unit network with Level 2,
- the unit network(s) with the other systems (if any),
- the external reference clock,
- the means to simulate the loads of the various networks, when these loads have been identified as possible influencing conditions.

The redundancy level of each component will be the one of the architecture to be qualified or assessed.

The system will be loaded with the minimum application capable to:

- handle all interface units installed,
- perform the application processing of all selected paths,
- generate the processing units load as defined during the system modeling (Section 7.4.4. influencing parameters).

7.7.2.2 Test System

The test system shall enable the generation of events on all the inputs of the selected paths, as well as the monitoring and recording of all corresponding events (and the accompanying dates) on the outputs of the selected paths.

This paragraph describes the general principles defining these generation and monitoring means. However, when preparing the test, it is recommended to check if the system under evaluation offers other means or "tricks" to generate or monitor these events.

7.7.2.2.1 Generation of Events on Paths Inputs

Possible inputs of selected paths are:

- direct LOG inputs,
- direct ANA inputs,
- network inputs (through fieldbus or unit network),

- Level 1 HMI inputs,
- inputs internal to the system (such as diagnostic variable).

In order to perform the time tagging absolute accuracy sub-tests, it is necessary to generate events on the inputs of the system which are perfectly "located" in the time of the external reference clock.

To achieve this, the method recommended for the direct (LOG or ANA) inputs consists in using an external reference clock which is capable (in addition to synchronizing the system) to deliver sync pulses which can be acquired by the system directly (i.e., avoiding interposing relays) through its standard interface units.

In the case of network inputs, there is no general and simple solution to generate events perfectly located in the time of the external reference clock. Unless the system under evaluation offers a specific solution, the paths having network inputs will be subject of time tagging relative accuracy sub-tests only.

In order to perform the time tagging relative accuracy sub-tests, it is necessary to have a signal generator capable to generate dynamic square signals, using programmed sequences, et delivered in parallel to the two inputs (LOG or ANA; direct or network) of all selected pairs of paths.

In the case of Level 1 HMI inputs, or inputs internal to the system, the events will be generated manually, and synchronized either with the external reference clock display, or with other manual event generations (and therefore with a weak accuracy, of the order of a few tenth of a second, and at a low rate).

7.7.2.2.2 Outputs Monitoring and Recording

Possible outputs of selected paths are:

- outputs to Level 2 system,
- outputs to Level 1 HMI,
- outputs to other systems.

In order to monitor and record these outputs, it is necessary to have:

- either a representative configuration of the actual system (Level 2 system, Level 1 HMI, other systems) to which the system under evaluation sends its outputs accompanied by a date,

- or a line spying device, capable to intercept all information sent to this system, along with accompanying dates.

In both case, it is essential to have a printing device, as well as a computer media storing device, in order to ensure the traceability and reproducibility of the test.

7.7.3 Time Tagging Absolute Accuracy Sub-Tests

7.7.3.1 Events Generation on the Inputs

As indicated above, these sub-tests are based on the injection of sync pulses delivered by the external reference clock on the input of the selected paths.

The periodicity of these sync pulses shall be chosen:

- high enough to be sure of the correspondence between an event on the path input, and the associated event on the path output,
- low enough to get a significant result on the duration of a repetition.

It is therefore recommended to choose a period between 1 second and one minute.

In case of manual generation (Level 1 HMI inputs, or "internal" inputs), only a few events will be generated without any specific period.

The duration of a repetition is generally set to 5 minutes, except for measures covering influencing conditions whose impact exceeds this duration, for example:

- loss of external reference clock: the duration will be chosen long enough to estimate properly the drift, e.g., 48 hours (a week end),
- change of date or time: the duration will be chosen long enough to ensure that the system has stabilized,
- loss and reinsertion of a component: the duration will be chosen long enough to ensure that the system is fully resynchronized.

7.7.3.2 Readings

The following readings shall be recorded for each measure:

- the maximum and the minimum differences between the date accompanying the event on the path output, and the date of the sync pulse injected on the path input,
- the distribution of this difference on a few significant intervals.

7.7.4 Time Tagging Relative Accuracy Sub-Tests

7.7.4.1 Events Generation on the Inputs

As indicated above, these sub-tests are based on the parallel injection of the same signal on the two inputs of the selected pairs of paths. This signal shall have the following pattern:

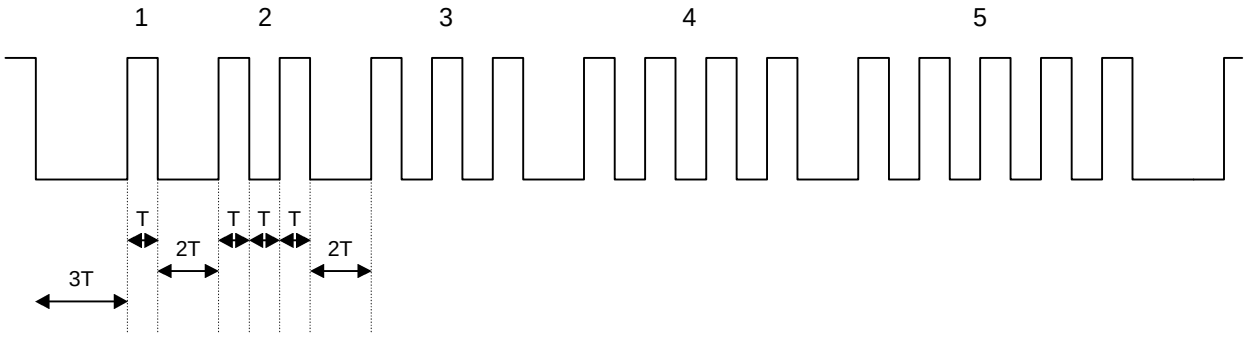


Figure B-13

(succession of sequences of 1, 2, 3, 4, 5 up and down transitions, separated by 3T)

In the case of LOG variables, the two levels correspond to 0 and 1. In the case of ANA variables, the two levels correspond to 25 and 75 % of the electrical or physical range.

This type of pattern ensures an easy correspondence between an event on an input, and the associated event on the output.

T is chosen close to 1 second, and not multiple of the system main acquisition or processing cycles.

The duration of a repetition complies with the same principles as for the time tagging absolute accuracy sub-tests. When the duration of a repetition exceeds a few minutes,

the same elementary sequences (1, 2, 3, 4, 5) are used, but are separated by a time larger than 3T.

7.7.4.2 Readings

The following readings shall be recorded for each measure:

- the maximum and the minimum differences between two dates accompanying the 2 events on the two path outputs associated to simultaneous events on the two path inputs,
- the distribution of this difference on a few significant intervals.

7.7.5 Analysis and Comparison with the System Modeling

The analysis of the readings will address for each sub-test:

- the comparison between the observed maximum dates differences, with the time tagging absolute and relative accuracies obtained by the system modeling, and verification of the impact of the influencing parameters on these time tagging accuracies.
- identification of dates differences which cannot be explained by the system modeling.
- identification of influencing conditions having a significant impact on the time tagging accuracy.

These analysis shall enable the confirmation of the system modeling, after possible modifications of this modeling and consultations with the system supplier.

7.8 Expected Results

The results expected from this test are of various natures, depending on the objectives this test fulfills:

- To understand and master the system, the test should insure:
  - — the validation of the system modeling,
  - — the validation of the system supplier data,
  - — the detection of possible system operation anomalies,

- To guide the system realization, the test should supply:
  - recommendations for the architecture design,
  - recommendations for the system configuration,
- To continue the system qualification (when applicable), the test should supply:
  - recommendations for possible additional analysis or simulation required to complete the (Level 1) control system evaluation,
  - recommendations for possible additional analysis or simulation required to complete the overall control system or the other control systems evaluations,
  - a list of additional information required from the supplier,
- To formally demonstrate the fulfillment of the requirements related to the time tagging characteristics, the test should confirm:
  - the time tagging absolute and relative accuracy for different paths or pairs of paths,
  - the main influencing parameters and conditions, and their impact on the time tagging accuracy.

8 Annex 1: Envelope Architecture Applied to a Few Off-the-Shelf Control Systems

Supplier	**Bailey**	**Cegelec**	**Foxboro**	
System	**Infi 90**	**P320**	**I/A S (Unix)**	**Contronic E**
Unit networks	Infinet	F900	NodBus	ABUS or SABUS LBUS (with Level 2)
Main rack	PCU	C370	Processor rack	
UC_0	NIS/NPM	S317, S319	CP or GW	CMX 40 (RUPI ABUS)
UT_1	NIS/NPM	UT120, S251, UT123	CP or GW	CMX40
UC_1	NIS/NPM	S316, S318	Fieldbus isolator	CMX 40 (RUPI PBUS)
Extension bus	Controlway	Locafip	Fieldbus	PBUS
Extension rack	MFP	CE2000	FBM rack	
UC_2	MFP	UT129	Fieldbus isolator	-
UT_2	MFP	UT129	-	-
UI	DSI, DSO, ASI, ASO, CIS	LE108, LE109 LD106,LC105A H115, AB120, AB121,AS111 AS112	FBM	PCARD