June 2, 1993

Mr. Alex Marion, Manager
Technical Division
Nuclear Management and Resources Council
Suite 300
1776 Eye Street, N.W.
Washington, D.C. 20006

Dear Mr. Marion:

The purpose of this letter is to thank you for your cooperation with the NRC staff on issues regarding digital instrumentation and control system upgrades, and to transmit the NRC staff comments on the draft "Guideline for Licensing Digital I&C Upgrades." The enclosed comments are in the form of strikeouts and redline of the original draft. The primary NRC staff concern, as discussed in our meeting on the 15th of April and as reflected in our comments, is the need to clearly establish a threshold for NRC staff review of certain digital I&C system upgrades, primarily based on the impact of software reliability and electromagnetic environment on the current plant safety analysis.

We look forward to future interactions with NUMARC, and are prepared to meet with you as necessary to discuss the proposed draft guideline at a mutually convenient time. Please feel free to contact me at (301) 504-2821 or Paul Loeser at (301) 504-2825 should you have any questions or comments.

Jared S. Wermiel, Chief
Instrumentation and Controls Branch
Division of Reactor Controls
and Human Factors

Enclosure:
As stated

DISTRIBUTION
Central File
HICB R/F
PDR
P. Loeser
J. Mauck
J. Wermiel
B. Boger
W. Russell

HICB	SC:HICB	BC:HICH	D:DRCH
PLoeser:lsh PL	JMauck	JWermiel	BBoger
6/2/93	6/2/93	6/2/93	6/2/93

Document Name: NRC-UPDT.LTR

DF03
1/1

TABLE OF CONTENTS

SECTION PAGE

Section 1 INTRODUCTION 1-1

1.1 BACKGROUND 1-1

1.2 PURPOSE 1-2

1.3 CONTENT OF THIS GUIDELINE 1-3

Section 2 DEFINITIONS AND TERMINOLOGY 2-1

Section 3 THE EXISTING LICENSING PROCESS AND 10CFR50.59 3-1

3.1 WHEN 10CFR50.59 APPLIES 3-1

3.2 REVIEW FOR POTENTIAL TECH SPEC CHANGES 3-1

3.3 PERFORMING THE 10CFR50.59 SAFETY EVALUATION 3-3

3.4 APPLICATION OF THE EXISTING LICENSING PROCESS TO DIGITAL UPGRADES 3-4

Section 4 GUIDANCE ON ADDRESSING DIGITAL UPGRADE ISSUES 4-1

4.1 SOFTWARE 4-2

4.1.1 Software Design and Quality Assurance 4-2

4.1.2 Software Common Mode Failures and Defense in Depth 4-3

4.2 EQUIPMENT QUALIFICATION INCLUDING EMI 4-6

4.3 MAN-MACHINE INTERFACE (MMI) 4-9

4.4 COMMERCIAL GRADE ITEM DEDICATION 4-10

4.5 DESIGN, SPECIFICATION, AND IMPLEMENTATION PROCESS 4-10

4.5.1 Definition of Systems, Interfaces, and Design Requirements 4-11

4.5.2 Plant-Specific Configurations and Optional Features 4-11

4.5.3 Design Specification 4-11

Section 5 SUPPLEMENTAL GUIDANCE FOR 10CFR50.59 EVALUATIONS OF DIGITAL UPGRADES 5-1

Section 6 REFERENCES 6-1

Section 1

INTRODUCTION

1.1 BACKGROUND

Nuclear utilities are now upgrading their existing analog instrumentation and control (I&C) systems. The upgrades are being driven primarily by the growing problems of obsolescence, difficulty in obtaining parts, and increased maintenance costs of the analog electronic systems. There also is great incentive to take advantage of modern digital technologies which offer potential performance and reliability improvements.

To assist the utilities in these upgrades, the Electric Power Research Institute (EPRI) has undertaken a number of activities as part of an overall Integrated I&C Upgrade Program. Preparation of this guideline is one of the activities. EPRI and the Nuclear Management and Resources Council (NUMARC) are coordinating industry interaction with the Nuclear Regulatory Commission (NRC) in providing guidance for licensing digital I&C upgrades. The goal of these activities is a well-defined, stable, and predictable regulatory framework which ensures that digital I&C system upgrades are accomplished in a safe and effective manner.

A number of issues have been identified related to the use of digital computer-based equipment in safety systems. These include the use of software and the potential for common mode failure resulting from software errors, the effect of electromagnetic interference on digital computer-based systems, the use and control of configuration equipment, and the commercial dedication of digital equipment including software. The most notable of these concerns is the use of software and potential software common mode failures.

The industry and NRC have recognized that it is important for digital I&C upgrades to go forward. Analog systems are continuing to become obsolete and difficult to support as vendors are discontinuing their lines of analog electronic equipment. Modern digital systems offer the potential to provide greater system reliability through the use of reliable digital components and features such as automatic self-testing and diagnostics. Assessment of system reliability should consider the effects of both the reliability enhancing features and the potential failure modes. When properly implemented, digital I&C upgrades can improve the safety of operating plants.

1.2 PURPOSE

The purpose of this document is to provide guidance that will assist utilities in accomplishing digital I&C upgrades within a stable licensing environment. The basic approach is to ~~follow the existing licensing process governed by 10CFR50.59.~~ establish a threshold, above which the digital upgrade is expected to fail the criteria of 10 CFR 50.59, therefore requiring prior Commission approval. For digital systems below the threshold, the utilities may determine, using the criteria of 10 CFR 50.59, that there is no unreviewed safety question, and no prior Commission approval is required. Some concerns stem from the design characteristics of the digital electronics which could result in new failure modes and system malfunctions that are considered unreviewed safety questions. These concerns include but are not limited to the use of software, the effect of electromagnetic interference, the use and control of configuration equipment, the effect that some digital designs have on diverse trip functions, failures specific to digital hardware, effective system integration, man-machine interface, and the commercial dedication of digital electronics. The most notable of these concerns is the use of software in a safety-related system.

The threshold concept does not alleviate the responsibility or authority of the licensee to perform an evaluation against 10 CFR 50.59 in every case of equipment upgrade or modification, nor does it predetermine the outcome. It is possible that in cases where one digital system is replacing another digital system, for example, that these issues have already been reviewed, and are therefore included in the licensing basis. It may also be that there is sufficient diversity in both hardware and software within a system that when a common mode software failure is assumed, diverse channels will cause the system to perform its intended function. In each case, it is the responsibility of the licensee to perform the 50.59 evaluation, and take action as appropriate.

It should be noted that for those cases where a licensee is proposing a modification to a design previously approved by the Commission, or references a design previously approved by a topical report evaluation, the scope of the NRC staff review would most likely be significantly reduced. In such cases, the NRC staff review would focus on plant specific issues (e.g. environmental effects, quality control plans, and any operating experience) and not reopen those generic concerns (e.g. software quality) previously reviewed and approved.

~~However,~~ This supplemental guidance is provided to facilitate the safety evaluation process for upgrades that use digital computers and software. This document provides guidance for:

- Performing and documenting 10CFR50.59 evaluations for digital upgrades, and
- Addressing the issues, noted above, that are associated with digital upgrades in safety systems.

The intent is that, if the utility follows the guidance provided in this document, the upgrade will satisfy licensing requirements with respect to the issues identified above, and the design will ultimately provide a safe and reliable system whether or not implemented with prior Commission approval is required.

1.3 CONTENT OF THIS GUIDELINE

Section 2 provides definitions for key terms used in the guideline. Section 3 describes the existing licensing process which is followed when making plant modifications, including evaluation for changes to the plant Technical Specifications and performing safety evaluations required by 10CFR50.59.

Section 4 describes the special considerations that apply to the licensing process for digital upgrades in safety systems. It provides guidance for addressing the issues of software, electromagnetic interference, man-machine interfaces, and commercial dedication. Section 5 provides supplemental guidance for performing a 10CFR50.59 safety evaluation for a digital upgrade.

Section 6 provides a list of documents which are referenced in this guideline and which provide supporting information and guidance. Appendix A provides additional background and examples in the form of case studies.

Section 2

DEFINITIONS AND TERMINOLOGY

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

Commercial grade item. An item which:

(a) is not subject to design or specification requirements that are unique to nuclear facilities;

(b) is used in applications other than nuclear facilities; and,

(c) is to be ordered from the manufacturer/supplier on the basis of specifications set forth in the manufacturer's published product description.

Commercial grade item dedication. A process of evaluating, including testing, and accepting commercial grade items to obtain adequate confidence in their suitability for safety application.

Computer. See programmable digital computer.

Computer program. A schedule or plan that specifies actions that may or may not be taken, expressed in a form suitable for execution by a programmable digital computer. [ANSI/IEEE-ANS 7-4.3.2-1982]

Configuration control. An element of configuration management consisting of the evaluation, coordination, approval or disapproval, and implementation of changes to configuration items after formal establishment of their configuration identification. [ANSI/IEEE 610.12-1990]

Data. A representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by a programmable digital computer. [ANSI/IEEE-ANS 7-4.3.2-1982]

Digital computer. See programmable digital computer.

Electromagnetic compatibility (EMC). The ability of equipment to function satisfactorily in its electromagnetic environment without introducing intolerable disturbances to that environment or to other equipment. [IEC 801-3-1984]

Electromagnetic interference (EMI). Electromagnetic disturbance which manifests itself in performance degradation, malfunction, or failure of electrical or electronic equipment. [IEC 801-3-1984]

Firmware. The combination of software and data that resides in read-only memory.

Integration tests. Tests performed during the hardware-software integration process prior to computer system validation to verify compatibility of the software and the computer system hardware. [ANSI/IEEE-ANS 7-4.3.2-1982]

Microprocessors. See programmable digital computer.

Programmable digital computer. A device that can store instructions and is capable of the execution of a systematic sequence of operations performed on data that is controlled by internally stored instructions. [ANSI/IEEE-ANS 7-4.3.2-1982]

Radio-frequency interference (RFI). A form of electromagnetic interference (EMI). EMI is a broader definition which includes the entire electromagnetic spectrum, whereas RFI is more restricted to the radio-frequency band, generally considered to be between 10 Khz and 50 Ghz. This term has been superseded by the broader term EMI.

Safety related. See safety systems.

Safety systems. Those systems that are relied upon to remain functional during and following design basis events to ensure (i) the integrity of the reactor coolant pressure boundary, (ii) the capability to shut down the reactor and maintain it in a safe shutdown condition, or (iii) the capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposures comparable to the 10 CFR Part 100 guidelines. [IEEE 603-1991]

Software. Computer programs and data. [ANSI/IEEE-ANS 7-4.3.2-1982]

Verification and Validation (V&V). The process of determining whether the requirements for a system or component are complete and correct, the products of each development phase fulfill the requirements or conditions imposed by the previous phase, and the final system or component complies with specified requirements. [IEEE 610.12-1990]

Section 3

THE EXISTING LICENSING PROCESS AND 10CFR50.59

As part of making a change to a nuclear power plant, the utility performs the necessary reviews and evaluations to ensure that the change is safe, verifies that the change meets the applicable regulations, determines the effect of the change on the plant's licensing basis, and determines whether licensing review or approval of the change is needed from the NRC. An important regulation that governs changes to a licensed nuclear facility is 10CFR50.59. This regulation gives the utility the prerogative to make changes to the plant without prior NRC review or approval, as long as a safety evaluation is performed and several conditions are met as spelled out in the regulation.

Specifically, under the provisions of 10CFR50.59 the licensee is allowed to (a) make changes in the facility as described in the Safety Analysis Report, (b) make changes in the procedures as described in the Safety Analysis Report, and (c) conduct tests or experiments not described in the Safety Analysis Report without NRC review and approval prior to implementation, provided the proposed change, test, or experiment does not involve a change in the Technical Specifications or is an unreviewed safety question. A proposed change, test, or experiment is considered to involve an unreviewed safety question (1) if the probability of occurrence or the consequence of an accident or malfunction of equipment important to safety previously evaluated in the Safety Analysis Report may be increased, or (2) if the possibility for an accident or malfunction of a different type than any previously evaluated in the Safety Analysis Report may be created, or (3) if the margin of safety as defined in the basis for any Technical Specification is reduced.

Figure 1 shows the process that typically is followed in performing safety reviews and addressing the licensing aspects of a proposed change. The figure is taken from NSAC-125. "Guidelines for 10CFR50.59 Safety Evaluations."[1]

3.1 WHEN 10CFR50.59 APPLIES

NSAC-125 provides detailed guidance for determining if the subject system is included in those for which 10CFR50.59 is applicable. As discussed in NSAC-125, 10CFR50.59 requires safety evaluations only for changes to the facility that affect the design, function, or method of performing the function of a structure, system, or component (SSC) described in the Safety Analysis Report (SAR) either by text, drawing, or other information relied upon by the NRC in granting the license. The intent is to require a safety evaluation for any modification that could affect the safety analysis. NSAC-125 provides examples for this determination and discusses issues such as distinguishing between a maintenance activity and a design change.

3.2 REVIEW FOR POTENTIAL TECH SPEC CHANGES

The determination of whether the upgrade involves a Technical Specification change can be made by a

[1] NSAC-125 is an industry guideline that has been used widely by utilities to develop their specific procedures for compliance with 10CFR50.59.

This chart is unchanged, and will be used as in NSAC-125

Safety Review Process
(From NSAC-125)
Figure 1

review of the Technical Specifications relative to the planned upgrade. The review should cover the items listed below:

- *Safety limits, limiting safety system settings, and limiting control settings*. These are limits upon important process variables that are found to be necessary to reasonably protect the integrity of certain of the physical barriers that guard against the uncontrolled release of radioactivity.

- *Limiting conditions for operation*. These are the functional capabilities or performance levels of equipment required for safe operation of the facility.

- *Surveillance requirements*. These are requirements relating to test, calibration, or inspection to assure that the necessary quality of systems and components is maintained, that facility operation will be within the safety limits, and that the limiting conditions of operation will be met.

- *Design features*. Design features to be included are those features of the facility such as time response and channel accuracy which, if altered or modified, could have a significant effect on safety.

- *Administrative controls*. These provisions relate to organization and management, procedures, record keeping, review and audit, and reporting necessary to assure operation of the facility in a safe manner.

The review should address the bases for the Technical Specifications and applicable plant Safety Evaluation Reports (SERs) to determine if any changes are needed. It should consider in particular any parameters or assumptions that may have been unique to the analog system and no longer apply with the digital upgrade. It should also include consideration of parameters or assumptions unique to digital systems that were not required for analog systems, and therefore need to be added.

If the planned upgrade involves a change to the Technical Specifications, then the licensee must submit a request for amendment to the facility license in accordance with the provisions of 10CFR50.90. The NRC must approve the Technical Specification change prior to implementation of the plant modification. The submittal should concentrate on those aspects of the modification that result in the Technical Specification change.

3.3 PERFORMING THE 10CFR50.59 SAFETY EVALUATION

NSAC-125 provides general guidance for preparation of a safety evaluation when it is required by 10CFR50.59. See Figure 1. The three questions posed by 10CFR50.59 are broken down to seven questions in NSAC-125 that are more specific and somewhat easier to address. The seven questions are explained and guidance is given on how to address them and determine whether the change involves an unreviewed safety question.

The possibility of a malfunction not previously evaluated in the final safety analysis report, and a possible reduction in the current sa.ety margin, calls into question the performance of an analog-to-digital modification of a safety system under the 10 CFR 50.59 rule. Therefore, for digital upgrades involving the Reactor Protection System (RPS), the Engineered Safety Features (ESF) control and actuation systems and systems which fall into the Post Accident Monitoring (PAM) category 1 items as defined in Regulatory Guide 1.97, application of 10 CFR 50.59 would lead to an unreviewed safety question and thus prior Commission approval of the change is required. This position is based upon the understanding that with the possibility of common mode software failure and increased sensitivity to the electromagnetic environment, and the high degree of importance to safety of these systems, an evaluation based on the 10 CFR 50.59 rule will show that new failure modes and thus an unreviewed safety question exists. Modifications to systems other than those mentioned above are below the threshold because of their lesser safety significance, and that after an evaluation against 10 CFR 50.59 guidelines is done, it may be that no Commission approval is required prior to implementation of the change. This determination will depend upon the outcome of the specific 10 CFR 50.59 evaluation.

If the change is determined to involve an unreviewed safety question, the licensee must request review and approval from NRC prior to implementation. The submittal should concentrate on those aspects of the change that result in the unreviewed safety question.

3.4 APPLICATION OF THE EXISTING LICENSING PROCESS TO DIGITAL UPGRADES

The process described above — determining when 10CFR50.59 applies, whether a modification involves a Technical Specification change, and whether it involves an unreviewed safety question based on the questions in 10CFR50.59 — applies to digital I&C upgrades as it does to other plant modifications. However, there are some additional special considerations that should be addressed when making digital I&C upgrades to safety systems. These special considerations address issues such as use of software and the potential for software common mode failures. The special considerations for digital upgrades are discussed in Section 4. Guidance for addressing them, within the context of the existing licensing process described above, is given in Sections 4 and 5.

In general, software cannot be thought of as an electronic component similar to other components installed in redundant channels that are physically and electrically separated from each other as was done with previously licensed analog design. Once a final software package is developed, this exact same package (component) may be installed in each redundant channel including any errors and failure mechanisms that may be induced by the software itself. With the same software component installed in each redundant channel or train of a safety system, the potential exists for a simultaneous failure in multiple safety trains. Such a failure would affect the ability of the safety system to perform its intended safety function. This concern is compounded by the use of portable configuration equipment that can alter the software in the field. As a result, the concern yields questions regarding the application of the single failure, independence, and separation criteria that were inherent in the original safety analysis. Furthermore, since some digital system designs use common information highways or can handle multiple input functions, a single digital equipment failure in one train could affect a number of the available trip functions thereby reducing the availability and functional diversity of existing designs.

Section 4

GUIDANCE ON ADDRESSING DIGITAL UPGRADE ISSUES

Section 1 listed several issues that have been identified with digital I&C upgrades in safety systems. These issues should be given special consideration in the design, specification, evaluation, and implementation of safety system digital upgrades. Specifically:

- The design and use of software should be given special attention, including verification and validation (V&V) and configuration management for software and the potential for software common mode failures.

- Qualification of computer-based equipment and demonstration of its compatibility with the environment should include consideration of electromagnetic interference (EMI) susceptibility and emissions.

- The potential for errors or inadvertent or unauthorized changes to be introduced via a man-machine interface (MMI) for computer-based equipment should be considered (e.g., via a configuration terminal, operator interface, or maintenance technician interface).

- Training / Personnel qualifications

- Commercial grade item dedication to qualify commercial grade digital equipment for use in safety systems should include consideration of software as well as hardware.

- Functional Diversity

- System Diversity requirements (i.e. ATWS)

This section describes how each of these issues can be addressed. The existing design basis issues from previous analog equipment which are applicable (i.e.; QA, seismic qualifications, redundancy, etc.) also need to be addressed. In many cases it draws on existing standards, regulatory requirements, and other sources of technical guidance, providing a summary or roadmap to these sources of guidance and discussing options the utility has for addressing the issues. Section 5 provides guidance on answering the 10CFR50.59 questions regarding potential unreviewed safety questions. It supplements the guidance that already is provided in NSAC-125, providing detailed questions that should be considered to address specifically the issues associated with digital I&C upgrades.

Section 3 discussed briefly the submittals that are required when the licensee determines that a modification involves a Technical Specification change or an unreviewed safety question. Note that it can be beneficial to inform the NRC early in the process, prior to determining what formal submittals may be required, about the intention to make a digital upgrade to a safety system. This can be informal, and it can help avoid misunderstandings and facilitate useful and timely interactions between the utility and NRC, potentially leading to a smoother licensing process for the upgrade.

4.1 SOFTWARE

4.1.1 Software Design and Quality Assurance

The design of digital computer-based I&C upgrades should place a high importance on software reliability and should include a well-defined process for software development, quality assurance, and configuration control.

Note that there may be several different types or categories of software involved in the upgraded system, with different organizations responsible for each. For example, the computer-based system may include:

- Base software delivered with the system (often as embedded firmware), developed by the vendor and sub-vendors — typically the vendor carries out the quality assurance, verification and validation of this software (e.g., for a programmable controller, the base software that implements the controller algorithms typically is unchanged from application to application);
- Application-specific software, including configuration information — if the utility is responsible for developing this software, it has the responsibility for its verification and validation (e.g., configuration data or software settings that configure selected algorithms of a programmable controller to implement the particular control application).

The ~~responsibilities~~ duties for development, V&V, and configuration control of the different portions of the software should be clearly specified. Also, required interactions between the utility and vendor in the development, review, and testing of the software should be specified. The utility should ensure that plant-specific or application-specific information needed by the vendor is adequately communicated and documented. Responsibility for the correct implementation and operation of the software rests on the licensee.

Standards, methods, and guidelines are available that allow the utility and the vendor to assure adequate software design, quality assurance, and verification and validation. Guidance for computer software development and integration of hardware and software for safety systems is provided in ANSI/IEEE-ANS 7-4.3.2. The 1982 revision of this standard was endorsed by Regulatory Guide 1.152, "Criteria for Programmable Digital Computer System Software in Safety-Related Systems of Nuclear Power Plants."

The following additional standards also can be used for guidance:

ASME NQA-2a-1990 Part 2.7	Quality Assurance Requirements of Computer Software for Nuclear Facility Applications
ANSI/IEEE 730-1989	IEEE Standard for Software Quality Assurance Plans
ANSI/IEEE 828-1990	IEEE Standard for Software Configuration Management Plans

ANSI/IEEE 830-1984	IEEE Guide to Software Requirements Specifications
ANSI/IEEE 1012-1986	IEEE Standard for Software Verification and Validation Plans
ANSI/IEEE 1016-1987	IEEE Recommended Practice for Software Design Descriptions
ANSI/IEEE 1028-1988	IEEE Standard for Software Reviews and Audits
ANSI/IEEE 1063-1987	IEEE Standard for Software User Documentation
IEC 880-1986	Software for Computers in the Safety Systems of Nuclear Power Stations

4.1.2 Software Common Mode Failures and Defense in Depth

Software reliability is a key element in the design of a digital computer-based I&C upgrade. Requirements and guidance provided in ANSI/IEEE-ANS 7-4.3.2 should be followed as discussed above to ensure that the software that is produced is of high quality and therefore reliable. Also, features such as automatic self-testing and diagnostics which are provided by modern software-based systems should be recognized for their potential to enhance system reliability. At the present time, however, there is a lack of consensus on methods for quantifying software reliability, particularly at the levels required of a safety system. As a result, there remain questions, particularly for relatively complex software-based systems, on the reliability of individual computers and the potential for a software common mode failure to cause a situation that is detrimental to plant safety.

~~The potential for s~~Software failures, including common mode failures, ~~should~~ shall be considered in the context of the overall assessment of system failure modes and the consequences of failures.~~—Note this assessment of failure modes should be conducted at the system level; it need not be a detailed evaluation of individual hardware or software component failures as long as the system level failure assessment bounds the credible failure modes for the system as a whole (e.g., fail high, fail low, or fail as is for system outputs).~~

A process that can be used to address software common mode failures is outlined below. Figure 2 provides a flowchart illustrating this process.

For each software failure that is considered:

1. ~~Assess whether the~~ Since it is considered impossible to prove that software is error free, software failure is deemed to be credible:

    - For simple systems which have extensive experience (both hardware and software), the measures taken to ensure software quality combined with successful operating experience gained with the system may be such that a software common mode failure

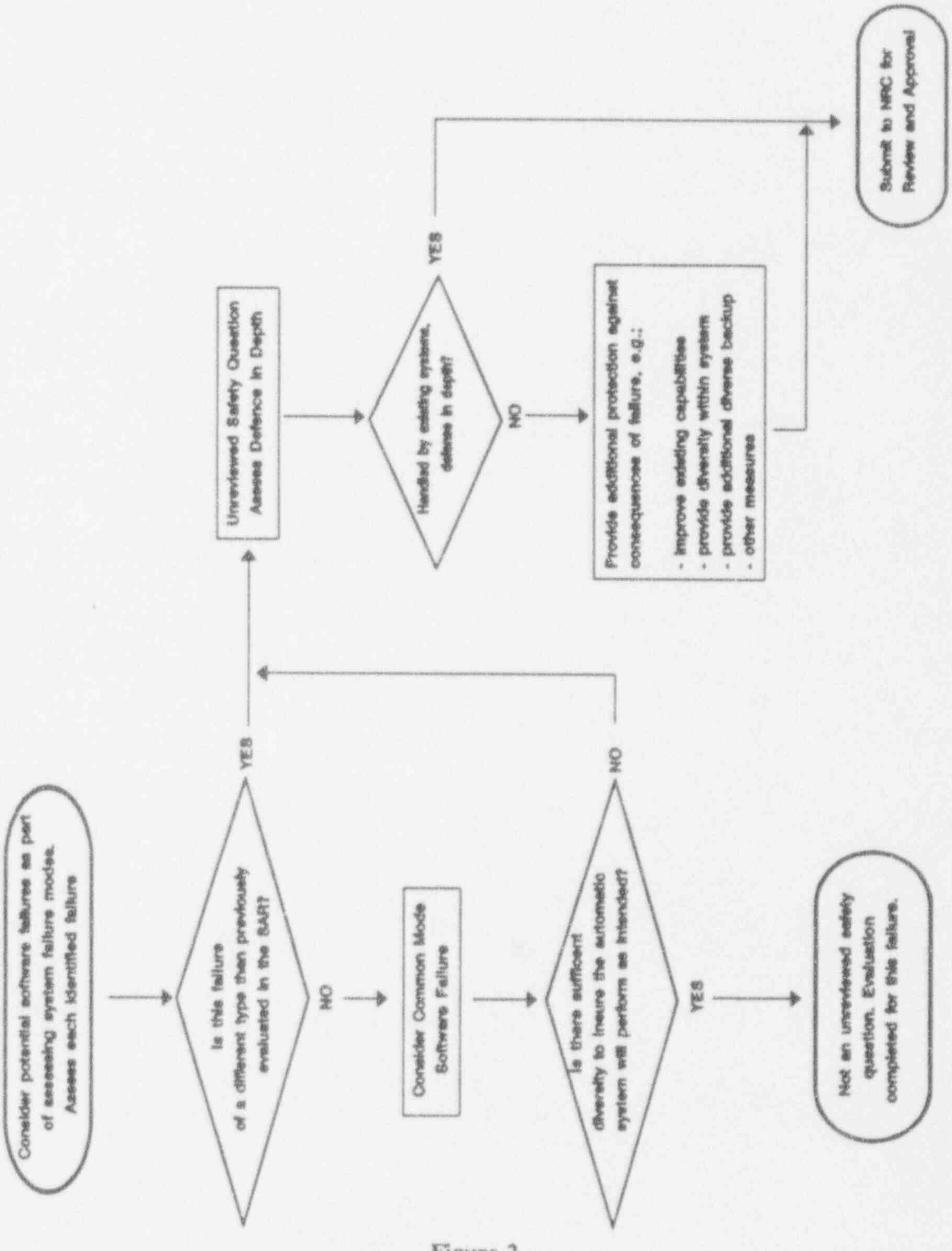
Consider potential software failures as part of assessing system failure modes. Assess each identified failure
Is this failure of a different type than previously evaluated in the SAR?
YES
NO
Consider Common Mode Software Failure
Is there sufficent diversity to insure the automatic system will perform as intended?
NO
YES
Not an unreviewed safety question. Evaluation completed for this failure.
Unreviewed Safety Question Assess Defence In Depth
Handled by existing system, defense in depth?
YES
NO
Provide additional protection against consequences of failure, e.g.:
- improve existing capabilities
- provide diversity within system
- provide additional diverse backup
- other measures
Submit to NRC for Review and Approval

Figure 2
Addressing Software
Common Mode Failure

is ~~not considered credible.~~ less likely, but is still credible. ~~Note that, for protection systems, the portion of the software that is critical to the system performing its safety functions is actually very simple because the functions it performs are simple (comparison of a signal to a setpoint, simple signal conditioning, etc.).~~

- For more complex systems or systems that have not seen extensive operating experience, software common mode failure may be ~~considered credible~~ more probable and, if so, should be given further evaluation (below).

2. ~~Assess the probability of the software failure, combined with probabilities of other events that also must occur (if any) for the consequences of the failure to be significant. For example, if the system under review is a backup system that must perform only when certain events occur, then a software failure in that system is important only if it could occur coincident with these other events producing the need for the backup system. It is important to assess the combined probabilities to place the failure in the appropriate context and determine whether it is meaningful.~~

~~If the probabilities are significant and warrant further consideration, then the consequences of the failure should be assessed (below).~~

~~3.~~ Assess the consequences of the software failure, assuming it does occur. Determine whether the consequences of the software failure represent ~~new type of system level failure that has not previously been considered.~~ an accident or malfunction of a different type than evaluated previously. It should be remembered that there is no guidance for quantitatively assessing software failure probabilities at this time. If the system under review is a backup system that must perform only when certain events occur, then a software failure in that system is important only if it could occur coincident with these other events producing the need for the backup system.

If the consequences of ~~the failure are not new and already have been addressed~~ a software failure of this type has already been evaluated and documented in the safety analysis report, then this particular failure need not be considered further. It would not represent an unreviewed safety question per 10CFR50.59.

However, if it is concluded that this is a new type of ~~system level~~ failure, then protection against the consequences of the failure ~~should~~ shall be considered (below). Note that this ~~typically~~ would mean the change involves an unreviewed safety question per 10CFR50.59 and NRC review and approval would be required prior to implementation.

43. Assess the defense in depth that is provided which would mitigate the effects of the plant design basis accidents ~~even~~ if the upgraded system suffered the software common mode failure. There are several options for demonstrating adequate defense in depth:

- Demonstrate that there is defense in depth with existing systems, procedures, and training which is adequate to mitigate the effects of the design basis accidents ~~even~~ if the upgraded system suffers the software common mode failure of concern -- this may include taking credit for operator action under defined circumstances, and it may include the use of nonsafety-related equipment, providing in either case, operator action or nonsafety equipment, the actions meet the safety analysis response time requirements and are independent and diverse from the proposed system design; or,

- Provide diversity within the upgraded system itself (e.g., diverse hardware and software in redundant portions of the system); or,
- Provide a separate backup system that gives adequate protection in the event of software common mode failure in the upgraded system.
- Provide a diverse monitoring system which will increase the likelihood of quickly identifying~~ identify~~ the occurrence of the common mode failure of the upgraded system, and provide guidance to the operators on their response to this failure.

4.2 EQUIPMENT QUALIFICATION INCLUDING EMI

10CFR50, Appendix A (GDC 2 and 4) requires that safety systems be designed to withstand the effects of natural phenomena and be qualified to operate in normal and postulated accident conditions. Environmental conditions that should be considered include temperature, pressure, humidity, seismic conditions, radiation, and electromagnetic interference (EMI).

As noted earlier, electromagnetic interference has been identified as an issue associated with digital I&C upgrades. The purpose of this section is to provide guidance and acceptable methods for addressing the EMI issue. It draws on a number of publications, such as IEEE Std 1050, Mil-Std 461 and 462, and ~~on guidance recently developed by EPRI and contained in~~ EPRI TR-102323.~~, "Guide to Electromagnetic Interference (EMI) Susceptibility Testing for Digital Safety Equipment in Nuclear Power Plants."~~

The EMI environment should be considered as part of the design basis conditions for the upgraded safety system. It should be shown that the equipment installed with the digital I&C upgrade will operate satisfactorily in the environment in which it is to be located. Key aspects of this evaluation are (1) knowledge of the plant EMI environment in which the equipment is expected to operate, (2) the execution of an appropriate set of tests to assess the vulnerability or susceptibility of the new equipment to EMI, (~~2~~3) the range of frequencies and test levels covered by the equipment susceptibility tests,~~ and~~ (~~3~~4) methods for demonstrating that the equipment is compatible with the EMI environment in which it will be installed, and (5) installation using proper grounding and shielding techniques. Each of these is discussed below.

~~The test methods specified in IEC 801-3, -4, and -5 which cover susceptibility to radiated field, electrical fast transients, and surges, supplemented by a low frequency conducted susceptibility test such as MIL-STD-461C, CS-01, are considered a comprehensive set of tests and an acceptable method for conducting EMI susceptibility testing. Alternate tests are identified in Table 1. These also are considered acceptable. Recommended signal levels and frequency ranges for the tests are provided in EPRI TR-102323.~~

~~Table 1~~

~~EMI Sources in a Nuclear Power Plant and Related Susceptibility Test Standards (from EPRI TR 102323)~~

~~Electromagnetic Interference~~ Signal	~~Origin~~	~~Related Susceptibility Test Standard~~
~~Continuous high frequency radiated~~	~~Walkie talkies; commercial radio; television transmitters; cellular phones; security systems~~	~~MIL-STD 461C&D, RS03, Class A3 Equipment in Ground Facilities; or IEC 801-3, or IEEE ANSI C63.12 (Guide)~~
~~Continuous low frequency conducted~~	~~Power distribution coupling between cables or grounds, includes surges due to faults~~	~~MIL-STD 461C, CS 01, RS 02, Part II, Class A3 Equipment in Ground Facilities; or IEC 801-6 (Draft)~~
~~Continuous high frequency conducted~~	~~Excitation of conductors/cables as RF transmission lines. Also coupling from signal generators and AC inverter switching spikes~~	~~MIL-STD 461C, CS 02 Class A3 Equipment in Ground Facilities; or MIL-STD 461D, CS 114 Class A3 Equipment in Ground Facilities; or IEC 801-6 (Draft), or IEEE ANSI C63.12 (Guide)~~
~~Transients Surges (high energy, infrequent)~~	~~Lightning or power fault effects on power distribution system and externally run cables~~	~~MIL-STD 461C, CS 06, Class A3 Equipment in Ground Facilities; or MIL-STD 461D, CS 116, Class A3 Equipment in Ground Facilities; or IEC 801-5, or IEEE ANSI C62.45~~
~~Transients, impulses & bursts of impulses (low energy, frequent)~~	~~Switching transients, inductive spikes on any control signal or power circuit. Secondary effects appear as damped sine wave or ringing~~	~~MIL-STD 461C, CS 06, RS 02 Part I, Class A3 Equipment in Ground Facilities; or MIL-STD 461D, CS 115, Class A3 Equipment in Ground Facilities; or IEC 801-4~~

~~Note that electrostatic discharge (ESD) is a localized phenomenon. When separation between redundant circuits is provided per IEEE 384, endorsed by Reg. Guide 1.75, then ESD is not considered a credible common mode failure initiator. ESD testing should be considered as part of equipment testing when separation between redundant circuits is not provided.~~

There are a number of standards and test methods, which if properly applied, will provide satisfactory results. Among these are the IEC 801 series and MIL-STD 461 and MIL-STD 462. The MIL-STD 461C susceptibility requirements are shown in the table below. In any of these, care must be taken to insure the entire frequency spectrum is covered. Ideally, frequencies considered should cover from 30 Hz to 20 GHz. 30 Hz is the first subharmonic of both the 60 Hz generated power and the supply voltage for most of the plant equipment. While this has a very long wave length, on the order of 3000 miles, and as such there is a low incidence of coupling, 60 Hz is the most common frequency in the plant, and therefore even a small degree of coupling can cause problems. 60 cycle hum on ground lines is not an unusual problem. 20 GHz is the upper end of the microwave spectrum, and may be used for point to point communications systems, both on-site and off site. The power levels in this frequency are usually much lower, but the short wavelengths may make even short wires a good antenna. The spectrum between 10 GHz and 20 GHz need be considered only if microwave systems using these frequencies are in the proximity of the plant. There must be a justification for any other frequencies not considered.

Applicable MIL-STD-461C susceptibility requirements for digital equipment	
Requirement[*]	Description
CS01	Conducted susceptibility, power leads, 30 Hz to 50 kHz
CS02	Conducted susceptibility, power and interconnecting control leads, 50 kHz to 400 MHz
CS06	Conducted susceptibility, spikes, power leads
RS01	Radiated susceptibility, magnetic field, 30 Hz to 50 kHz
RS02	Radiated susceptibility, magnetic and electric fields, spikes and power frequencies
RS03	Radiated susceptibility, electric field, 14 kHz to 20 GHz

[*] C = conducted, R = radiated, and S = susceptibility.

Site specific problems should be considered. These may include the frequency of any microwave systems installed on-site, or which is offsite but geographically close. Of specific interest is the handheld radio communications devices used by plant personnel. In addition, radar frequencies should be considered, both from local airports and shipboard radars for sites close to large bodies of water. Sites close to military bases should consider those radars.

In demonstrating that the equipment is compatible with the EMI environment in which it will be installed, there are several options:

1. ~~Using the test methods discussed above, qualify the equipment to conservative levels that can be shown to be greater than what is credible for the installed environment; a local site survey is not required in this case --- EPRI TR 102323 can be consulted to establish the levels for testing (see discussion below); or,~~

~~2. Demonstrate that the existing equipment is more susceptible than the new equipment to be installed with the upgrade — in some cases existing analog instrumentation has greater susceptibility to EMI than the modern digital equipment that is installed in its place; or,~~

~~3.~~ Perform local tests or surveys to measure the actual environment in which the equipment will be installed, and compare this to the results of the vendor or laboratory tests of equipment susceptibility; show that the equipment testing envelopes the installed environment.

2. Perform an analysis based on previous local tests or surveys, and the known emissions of any equipment added since that test, and compare this to the results of the vendor or laboratory tests of equipment susceptibility; show that the equipment testing envelopes the installed environment.

~~The EPRI Guide, TR-102323, contains qualification test options and test signal characteristics, including frequency range and magnitude, based on maximum expected interference levels determined by analysis and test. The EPRI Guide contains upper bounds for interference levels for all the EMI concerns noted in Table 1 and is applicable to any nuclear power plant.~~

Experience in previous upgrades has shown that wiring practices followed in installation of the equipment (e.g., routing, shielding, grounding, termination) are very important in minimizing EMI susceptibility and should be addressed in the design and implementation of the upgrade. IEEE 1050-1989 provides guidance in this area.

4.3 MAN-MACHINE INTERFACE (MMI)

The man-machine interface includes all interfaces between the digital I&C system and plant personnel, including:

- operators — alarms, status displays, control interfaces, etc.
- maintenance technicians — test and calibration interfaces, diagnostic information displays, data entry terminals for setpoints, etc.
- engineering personnel — configuration workstations or terminals, etc.

The principal concern related to the man-machine interface is the possibility of system failure due to human error, or due to unauthorized entries or alterations of the system through a maintenance, test, or configuration interface. Human factors considerations should be addressed in the design of all man-machine interfaces associated with the upgrade in order to minimize the possibility for human error in using the interface. IEEE 603-1991 discusses the application of human factors considerations in the design process for safety systems. General guidance for human factors considerations is provided in numerous IEEE, EPRI, and NUREG documents on this subject.

Adequate administrative controls and security should be provided to ~~guard against~~ prevent unauthorized changes being introduced through a man-machine interface. Note that this is similar to the situation that is faced now with existing equipment and the associated administrative controls and security (e.g., authorization to open cabinets, use of keylock controls, restrictions on vital area access, etc.). IEEE 603-1991 provides guidance on access control and human interfaces. Administrative controls and design features should specifically address software access in addition to typical equipment access provisions.

4.4 COMMERCIAL GRADE ITEM DEDICATION

The responsibilities for qualifying, or performing commercial dedication, of equipment for use in a safety system should be specified. This includes software as well as hardware. Note that, depending on how the roles are defined, the utility may need access to the source code for the vendor software. If so, this needs to be worked out up front (schedule, terms, etc.) so that the necessary reviews or dedication activities can be supported in a timely fashion.

The process used for commercial grade item dedication should identify the principal performance requirements necessary to provide adequate confidence that the safety function can be achieved. The hardware and software design should be compared to the applicable design criteria for nuclear qualified equipment~~, with exceptions taken where there are other compensating factors (e.g., documented operating experience in a similar application, or additional verification and validation performed to develop adequate confidence)~~. While documented operating experience can be used as a factor in commercial grade dedication, it is in itself insufficient as proof of acceptability for applications important to safety. Acceptance typically will be based on~~ adequate~~ a high degree of confidence that the product will not only perform its intended functions, but also that no unintended functions will occur. The degree of confidence required will be commensurate with the safety function the hardware and software is required to perform. Since for any reasonably large software package the number of input variables makes dedication by testing alone a very difficult proposition, the only viable alternative is to verify and validate the code itself, in addition to test. In a proprietary software product, the vendor may be reluctant to make the code listings available. For this reason, commercial dedication of software remains a limited option. Documentation and software required to maintain the commercial grade dedication~~ should~~ shall be placed under configuration management.

EPRI NP-5652, "Utilization of Commercial Grade Items in Nuclear Safety Related Applications," provides guidance on commercial grade item dedication.

4.5 DESIGN, SPECIFICATION, AND IMPLEMENTATION PROCESS

For digital I&C system upgrades, it is particularly important to establish early in the process the roles, responsibilities, and interfaces among the utility, equipment vendor, and other organizations that may be involved in the change. When the upgrade involves computers and software, responsibilities for verification and validation (V&V), testing, and configuration management for the different types of software (e.g., vendor-supplied firmware, software configuration data, etc., as discussed in 4.1.1 above) should be established up front. The ultimate responsibility for the correct operation of the system cannot, of course, be delegated, and as such, remains with the licensee.

Experience in previous digital upgrades and lessons learned from software development and use in general have shown that proper specification of the requirements for the software is a key element in assuring adequate performance of the system. Most problems with digital systems occur in specifying the system, not in implementing the system or the software. The process should be very thorough in establishing the requirements for the upgraded system, identifying all interfaces and all the applicable design basis requirements, and the utility should ensure that it adequately communicates to the vendor the plant-specific requirements and information needed to implement the system.

NSAC-105, "Guidelines for Design and Procedure Changes in Nuclear Power Plants," provides general guidance on design and implementation of plant modifications. IEEE 830-1984, "Guide for Software Requirements Specifications." provides more detailed guidance on the process of generating the software requirements specifications. Additional guidance related to specification of digital I&C upgrades is given below, supplementing the guidance contained in NSAC-105.

4.5.1 Definition of Systems, Interfaces, and Design Requirements

The systems that will be involved in the upgrade should be clearly defined. This includes defining:

- Objective(s) of the modification. For example, is this a functionally equivalent replacement or is additional functionality to be provided as part of the modification? This can have a significant impact on the safety evaluation.

- System(s) to be modified. What systems will be modified to support the objectives?

- Other systems affected. What are the effects from this modification on other systems? What interfaces are affected?

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

4.5.2 Plant-Specific Configurations and Optional Features

The utility should specify the particular options, features, and plant-specific configurations that are to be implemented for the particular design. The flexibility and power of computer-based systems allow a wide range of optional features and capabilities that the utility may or may not want in a particular application. In some cases, it may be desirable to disable or remove unnecessary optional capabilities, particularly if they open up the possibility of new types of malfunctions or misoperations that impact the safety evaluation.

Also, the utility should understand what actions it must take to properly implement the desired capabilities. An example is the area of self-testing, diagnostics, and fault detection. The equipment may support these features, but the vendor may rely on site-specific or customer-specific wiring or interfaces to fully implement them (e.g., the equipment provides a contact output that signals failure of a processor, and this contact must be wired to a separate system or other equipment to provide operator notification or maintenance action). Communication between the utility and the vendor is important in ensuring that these items are properly addressed in the design and installation.

4.5.3 Design Specification

Section 2 of NSAC-105 and IEEE 1016-1987, "Recommended Practice for Software Design Descriptions", provides guidance on preparation of a design specification. As noted above, the specification is a key element in ensuring adequate performance of the upgraded system. The specification should cover:

- Design objectives
- Functional requirements
- Codes, standards, and other design basis documents
- Design requirements
- Analysis and testing requirements
- Acceptance criteria

Section 5

SUPPLEMENTAL GUIDANCE FOR 10CFR50.59 EVALUATIONS OF DIGITAL UPGRADES

NSAC-125 provides a set of seven questions commonly used to determine if a modification involves one or more unreviewed safety questions in accordance with 10CFR50.59. If the modification involves an unreviewed safety question, NRC review and approval must be obtained prior to implementation.

It is important to remember that the 10CFR50.59 Safety Evaluation does not determine whether or not a proposed change is safe. A determination that a proposed change involves an unreviewed safety question does not mean that the change is unsafe. It simply means that NRC review and approval is necessary prior to implementation of the change.

The following provides items to consider in answering each of the seven questions referred to in NSAC-125. They are expressed in the form of supplemental questions. ~~It is important to keep in mind that an answer of "yes" or "no" to a given question does not automatically mean that there is or is not an unreviewed safety question. These are items to consider, not absolutes. Also, note that for a particular upgrade, some of the items listed may be more appropriately addressed under a different question or in several of the questions.~~ If any of these questions is answered "yes", the change is an unreviewed safety question (Section 4.2 of NSAC-125). It is important to ensure that all items are addressed fully and that all valid potential unreviewed safety questions are identified.

(1) *May the proposed activity increase the probability of occurrence of an accident evaluated previously in the Safety Analysis Report (SAR)?*

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

(a) Does the replacement system exhibit performance characteristics, or have design features, that give an increased probability of a system malfunction resulting in an accident? The assessment of a change in probability may be made on a qualitative basis, particularly for systems or components which rely on software since there does not currently exist a consensus method for quantifying software reliability. Common mode and common cause failures of software shall be considered. Section 3.4 of NSAC-125 provides guidance on the use of qualitative probability assessments.

(b) Does the system exhibit performance characteristics that require additional operator intervention for continued normal operation (e.g., lockup, halt)? It should also be noted that lockup or halt may be new types of malfunctions, and should be addressed under item 6 of this section.

(c) Is the system qualified for the installed environment (e.g., temperature, humidity, electromagnetic fields, airborne particulates) such that system performance will not be degraded compared to the original system?

(2) *May the proposed activity increase the consequences of an accident evaluated previously in the SAR?*

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

(a) Does the replacement system exhibit a response time beyond current acceptance limits (e.g., because of sample period, increased filtering)?
(b) Does the system perform adequately under high duty cycle loading (e.g., computational burden during accident conditions)?
(c) Does the architecture of the system exhibit a single failure that results in more severe consequential effects (e.g., reduced segmentation due to combining previously separate functions, several input channels sharing an input board, central loop processor for many channels)?
(d) Does the man-machine interface design introduce constraints on the operators' ability to adequately respond to an accident such that there are more severe consequential effects?

(3) *May the proposed activity increase the probability of occurrence of a malfunction of equipment important to safety evaluated previously in the SAR?*

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

(a) Does the modified system meet the required plant environmental and seismic envelopes?
(b) Is the replacement system qualified for the electromagnetic fields at the installed location? What effect does plant equipment operation have on the system (e.g., walkie talkies, motors, switchgear, etc.)?
(c) Have potential interactions between safety-related and nonsafety-related systems been addressed?
(d) Are the electrical loads associated with the replacement system addressed in the design?
(e) Does the plant HVAC have adequate capacity for the thermal loads of the replacement system?
(f) Does the replacement system meet applicable requirements for separation, independence, and grounding?
(g) Does the microprocessor-based system have adequately qualified cabinet cooling?

(4) *May the proposed activity increase the consequences of a malfunction of equipment important to safety evaluated previously in the SAR?*

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

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

(b) ~~Is~~ Since a software common mode failure (CMF) is a credible failure mode~~[2]? If so~~, are the consequences mitigated by the hardware design or system architecture? If not, is the probability of a software CMF in conjunction with other concurrent events assumed in the safety analysis judged to be sufficiently high that the consequences of a malfunction previously evaluated are increased? Are the consequences bounded by other events evaluated in the SAR?

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

(d) Is the response of the replacement system on restoration of power different from that of the analog system being replaced?

(e) Does the man-machine interface (MMI) introduce failure modes different from those of the existing analog system? Is there an equivalent to the MMI in the system being replaced, or does the existence of a new type of equipment create a new type of failure?

(5) *May the proposed activity create the possibility of an accident of a different type than any evaluated previously in the SAR?*

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

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

(b) ~~Is a software common mode failure a credible failure mode? If so, a~~Are the consequences of a software common mode failure mitigated by the hardware design or system architecture? Could the failure cause a different type of accident than presented in the SAR?

(c) Plant SAR analyses were based on credible failure modes of analog equipment. Does the replacement system change the basis for the most

[2] ~~Considerations in determining whether a software common mode failure is credible include (1) the complexity of the computer system design, (2) the number, size and complexity of the software programs involved, and (3) experience with the computer system and software.~~

limiting scenario?

(6) *May the proposed activity create the possibility of a malfunction of equipment important to safety ~~when the malfunction is~~ of a different type than any evaluated previously in the SAR?*

~~These areas should be addressed in responding to the question:~~

~~(a) Have assessments of system level failure modes and effects for the microprocessor based system identified any new types of failure that would result in effects not previously considered in the SAR?~~
~~(b) Is a software common mode failure a credible failure mode? If so, would it result in effects not previously considered in the SAR?~~
~~(c) Could the environment in which the microprocessor based equipment operates cause a new type of failure (e.g., electromagnetic susceptibility)? Could the new system create an environment which adversely affects other equipment and thereby creates the possibility of a different type of malfunction?~~
~~(d) Are the system design, verification and validation, and analysis methods consistent with industry standards?~~

This question is asking if the digital equipment could lead to a failure mode of a different type than the types evaluated in the SAR. In answering this question, the types of failure modes of the analog system being replaced that have been previously evaluated in the SAR and that are affected by the replacement are identified. Then types of failure modes that the digital replacement system could create are identified. Comparing the two lists can provide the answer to the question (NSAC 125 § 4.2.6).

(7) *Does the proposed activity reduce the margin of safety as defined in the basis for any technical specification?*

A review of the bases and assumptions for the Technical Specifications and acceptance limits spelled out in the NRC SERs should be made to support this determination. The areas to be addressed include the following:

(a) Has the replacement I&C system decreased the channel trip accuracy beyond the acceptance limit?
(b) Has the replacement I&C system increased the channel response time beyond the acceptance limit?
(c) Has the replacement I&C system decreased the channel indicated accuracy beyond the acceptance limit?
(d) Does the new control system cause a plant parameter for any analyzed event to fall outside of acceptance limits?

Section 6

REFERENCES

The following lists standards, guidelines, and other documents that are referred to in this guideline.

The EPRI Instrumentation & Control Requirements and Standards (ICRS) database, distributed by EPRI's Electric Power Software Center, can be consulted for more information on standards, regulatory documents, and guidelines related to I&C upgrades in nuclear power plants.

1. ASME NQA-2a-1990, Part 2.7, "Quality Assurance Requirements of Computer Systems for Nuclear Facility Applications," American Society of Mechanical Engineers.

2. ANSI/IEEE-ANS-7-4.3.2, "Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations."

3. ANSI/IEEE 384-1977, "Criteria for Independence of Class 1E Equipment and Circuits."

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

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

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

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

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

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

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

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

12. ANSI/IEEE 1050-1989, "IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations."

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

14. EPRI TR-102323, "Guide to Electromagnetic Interference (EMI) Susceptibility Testing for Digital Safety Equipment in Nuclear Power Plants." To be published by Electric Power Research Institute.

15. IEC 801-3, 1984, "Electromagnetic Compatibility for Industrial Process Measurement and

Control Equipment Part 3: Radiated Electromagnetic Field Requirements."

16. IEC 801-4, 1988, "Electromagnetic Compatibility for Industrial Process Measurement and Control Equipment Part 4: Electrical Fast Transient/Burst Requirements."

17. IEC 801-5, Draft, "Electromagnetic Compatibility for Industrial Process Measurement and Control Equipment Part 5: Surge Immunity Requirements."

18. IEC 801-6, Draft, "Electromagnetic Compatibility for Industrial Process Measurement and Control Equipment — Part 6: Immunity to Conducted Radio Frequency Disturbances Above 9 kHZ."

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

20. IEEE 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations."

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

22. NSAC-125, "Guidelines for 10CFR50.59 Safety Evaluations."

23. Regulatory Guide 1.152, "Criteria for Programmable Digital Computer System Software in Safety-Related Systems of Nuclear Power Plants."

24. Regulatory Guide 1.75, "Physical Independence of Electrical Systems."

25. Regulatory Guide 1.153, "Criteria for Power, Instrumentation and Control Portions of Safety Systems."

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

27. Title 10 of the Code of Federal Regulations, Part 50.90, "Application for Amendment of License or Construction Permit."