August 30, 1994

MEMORANDUM FOR: Dr. John T. Larkins, Executive Director
Advisory Committee on Reactor Safeguards

FROM: Elizabeth L. Doolittle, Acting Chief
Generic Communications Branch
Division of Operating Reactor Support
Office of Nuclear Reactor Regulation

SUBJECT: FORWARDING OF PROPOSED NRC GENERIC LETTER

Enclosed is a proposed NRC generic letter entitled, "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," for your information. The Committee for Review of Generic Requirements has endorsed noticing the proposed generic letter in the Federal Register for public comment. A copy of the proposed generic letter was forwarded to you on August 9, 1994, via a Frank J. Miraglia to Edward L. Jordan memo.

Original signed by
Elizabeth L. Doolittle, Acting Chief
Generic Communications Branch
Division of Operating Reactor Support
Office of Nuclear Reactor Regulation

Enclosure: As stated

Distribution:
Central Files PDR TJKim, NRR
BGrimes, NRR OGCB R/F EDoolittle, NRR

OFFICE	DORS:NRR	DORS:NRR
NAME	TJKim	BDoolittle
DATE	08/29/94	08/30/94

Enclosure

UNITED STATES
NUCLEAR REGULATORY COMMISSION
OFFICE OF NUCLEAR REACTOR REGULATION
WASHINGTON, D.C. 20555

(date)

NRC GENERIC LETTER 94-XX

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

Addressees

All holders of operating licenses or construction permits for nuclear power reactors.

Purpose

The U.S. Nuclear Regulatory Commission (NRC) staff is issuing this generic letter to inform addressees of a new staff position on the use of Nuclear Management and Resources Council/Electrical Power Research Institute (NUMARC/EPRI) Report TR-102348, "Guideline on Licensing Digital Upgrades," dated December, 1993, as acceptable guidance for determining when an analog-to-digital replacement can be performed without prior NRC staff approval under the requirements of Section 50.59 of Title 10 of the Code of Federal Regulations (10 CFR 50.59). The report applies to all digital equipment that uses software and, in particular, to microprocessor-based systems. The report, together with the clarifications discussed in this generic letter, represents a method acceptable to the staff for use in making a determination of whether or not an unreviewed safety question exists with respect to 10 CFR 50.59 requirements. It is expected that recipients will consider the information in this generic letter when performing analog-to-digital instrumentation and control systems replacements. However, suggestions contained in this generic letter are not NRC requirements; therefore, no specific action or written response is required.

Description of Circumstances

The age-related degradation of some earlier analog electronic systems and the difficulties in obtaining qualified replacement components for those systems, as well as a desire for enhanced features such as automatic self-test and diagnostics, greater flexibility, and increased data availability have prompted some operating reactor licensees to replace existing analog systems with digital systems. After reviewing a number of these digital system replacements and digital equipment failures in both nuclear and non-nuclear applications, the staff has identified potentially safety significant concerns pertaining to digital systems in nuclear power plants. The concerns of the staff stem from the design characteristics specific to the new digital electronics that could result in failure modes and system malfunctions that

either were not considered during the initial plant design or may not have been evaluated in sufficient detail in the safety analysis report. These concerns include potential common mode failures due to (1) the use of common software in redundant channels, (2) increased sensitivity to the effects of electromagnetic interference, (3) the improper use and control of equipment used to control and modify software and hardware configurations, (4) the effect that some digital designs have on diverse trip functions, (5) improper system integration, and (6) inappropriate commercial dedication of digital electronics.

As a result of the above concerns, the NRC staff issued a draft generic letter for public comment in the Federal Register (57FR36680) on August 14, 1992, wherein a position was established that essentially all safety-related digital replacements result in an unreviewed safety question because of the possibility of the creation of a different type of malfunction than those evaluated previously in the safety analysis report. The staff concluded, therefore, that prior approval by the NRC staff of all safety-related digital modifications was necessary. However, subsequent discussions and comments on the draft generic letter have resulted in the staff position as described in this letter.

Discussion

To assist licensees in effectively implementing digital replacements by addressing the concerns indicated above and in determining which upgrades can be performed under 10 CFR 50.59 without prior NRC staff approval, Report TR-102348 has been published. The NRC staff reviewed and provided comments on this report while it was in draft form, and the final report reflects a coordinated effort between industry and the NRC staff. The NRC staff believes that, when properly implemented, modern digital systems offer the potential for greater system reliability and enhanced features such as automatic self-test and diagnostics, as well as greater flexibility, increased data availability, and ease of modification.

Report TR-102348 contains guidance that will assist licensees in implementing and licensing digital upgrades in such a manner as to minimize the potential concerns indicated above. It describes actions to be taken in the design and implementation process to ensure that the digital upgrade licensing and safety issues are addressed, and ways to consider these issues when performing the 10 CFR 50.59 evaluation. It is not the intent of the report or of the NRC staff to predispose the outcome of the 10 CFR 50.59 process, but rather to provide a process that will assist licensees in reaching a proper conclusion regarding the existence of an unreviewed safety question when undertaking a digital system replacement. However, as shown in Example 5-6 of the report, when using this document as guidance for the analysis of modifications of some safety-significant systems such as the reactor protection system or an engineered safety feature system, it is likely these digital modifications will require staff review when 10 CFR 50.59 criteria are applied.

Report TR-102348 states in the introduction that the guidance is supplemental to and consistent with that provided in NSAC-125, "Guidelines for 10 CFR 50.59

Safety Evaluations." Licensees should bear in mind that NSAC-125 has not been endorsed by the NRC, and therefore any use of those guidelines is advisory only, and that nothing in NSAC-125 can be construed as a modification of 10 CFR 50.59. While the guidelines of NSAC-125 can be useful in the evaluation of systems, and are representative of logic used in making a 10 CFR 50.59 determination, the actual determination of whether or not an unreviewed safety question exists must be done in accordance with 10 CFR 50.59.

10 CFR 50.59(a)(2)(i) and (ii) states that a proposed change, test or experiment involves an unreviewed safety question if the probability or consequences of an accident or malfunction previously evaluated in the safety analysis report may increase, or if the possibility for an accident or malfunction of a different type than any previously evaluated in the safety analysis report may be created. If during the 10 CFR 50.59 determination there is uncertainty about whether the probability or consequences may increase, or whether the possibility of a different type of accident or malfunction may be created, the uncertainty should lead the licensee to conclude that the probability or consequences may increase or a new type of malfunction may be created. If the uncertainty is only on the degree of improvement the digital system will provide, the modification would not involve an unreviewed safety question. If, however, the uncertainty involves whether or not this modification is more or less safe than the previous analog system, or if no degree of safety has been determined, an unreviewed safety question is involved.

The staff believes that two clarifications to Report TR-102348 are appropriate as follows:

1. 10 CFR 50.59 requires determination of whether "a possibility for an accident or malfunction of a different type than any previously evaluated in the safety evaluation report may be created." As a part of this determination, Report TR-102348 suggests looking for "any new types of system-level failures that would result in effects not previously considered in the FSAR." (For example, see TR-102348, Section 4.5, Question 6.) It is the NRC staff's position that the system-level considered in this regard should be the digital system being installed. The staff believes that this clarification is necessary because 10 CFR 50.59 does not refer to "system-level" failure but rather refers to the malfunction of the equipment important to safety being modified. As an example, when installing an upgraded digital high pressure function of the reactor trip system, it is the digital instrumentation and control circuitry associated with the high pressure reactor trip function that would be subject to the questions on failure modes and effects identified in the report that would represent the unreviewed safety question, not the entire reactor trip system. If the entire trip system is being replaced with a digital upgrade, then the entire replacement digital instrumentation and control system would be subject to the failure modes [illegible] cts analysis, not the full range instrumentation and control systems being actuated to respond to a transient or accident.

2. 10 CFR 50.59 requires maintaining records that "include a written safety evaluation which provides the bases for the determination that the change, test, or experiment does not involve an unreviewed safety question." Section 3.1.2 of the report points out that the use of qualitative engineering judgment is typically involved in areas that are not readily quantifiable, such as likelihood of the failure, its importance to the system and to the plant, and the practicality and incremental improvements of various options available for resolving the failure. Such judgments may be difficult to duplicate and understand at a later time. It is the NRC staff's position that the basis for the engineering judgment and the logic used in the determination should be documented to the extent practicable. This type of documentation is of particular importance in areas where no established consensus methods are available, such as for software reliability, or the use of commercial-grade hardware and software where full documentation of the design process is not available.

EPRI Report TR-102348, together with the clarifications discussed in this generic letter, can be used as guidance by licensees in both designing analog-to-digital replacements and, with respect to unreviewed safety question determinations, determining if an analog-to-digital replacement can be performed under 10 CFR 50.59 without prior staff approval.

This generic letter requires no specific action or written response. If you have any questions about this matter, please contact the technical contact listed below or the appropriate Office of Nuclear Reactor Regulation project manager.

Roy P. Zimmerman
Associate Director for Projects
Office of Nuclear Reactor Regulation

Technical contact: Paul J. Loeser, NRR
(301) 504-2825

Lead project manager: Robert M. Pulsifer, NRR
(301) 504-3016

Attachment:
List of Recently Issued NRC Generic Letters