UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

NOV 16 1984

MEMORANDUM FOR: Bill M. Morris, Chief
Electrical Engineering Branch
Division of Engineering Technology, RES

FROM: Zoltan R. Rosztoczy, Chief
Division of Safety Technology, NRR

SUBJECT: NRR COMMENTS ON REGULATORY GUIDE TASK IC 127-5, "CRITERIA FOR PROGRAMMABLE DIGITAL COMPUTER SYSTEMS SOFTWARE IN SAFETY RELATED SYSTEMS OF NUCLEAR POWER PLANTS"

This proposed Regulatory Guide had been approved previously by NRR for submittal to ACRS and release for public comment. RES has subsequently incorporated appropriate ACRS and public comments.

The enclosed version has been reviewed within ICSB/DSI, SPEB/DST, and HFEB/DHFS. The NRR review has produced some minor revisions which have been marked on the enclosed version. The value/impact statement was also updated.

We recommend that RES prepare a version based on the enclosed marked copy for CRGR review. Mr. Faust Rosa will represent the principal NRR user division (DSI) during the CRGR meeting when the subject guide is discussed.

Richard Clarke
for Zoltan R. Rosztoczy, Chief
Research and Standards Coordination Branch
Division of Safety Technology, NRR

Enclosure:
Marked Versions of
Regulatory Guide Task IC 127-5
and Value/Impact Statement

ENCLOSURE

U.S. NUCLEAR REGULATORY COMMISSION
OFFICE OF NUCLEAR REGULATORY RESEARCH

June 6, 1984
~~March 1983~~
Division 1
Task IC 127-5

~~DRAFT~~ REGULATORY GUIDE AND VALUE/IMPACT STATEMENT

Contact: ~~D. W. Deehm~~ A. S. Hintze (301)443-~~5966~~ 7690

CRITERIA FOR PROGRAMMABLE DIGITAL COMPUTER SYSTEMS SOFTWARE -RELATED IN SAFETY SYSTEMS OF NUCLEAR POWER ~~GENERATING STATIONS~~ PLANTS

A. INTRODUCTION

Criterion 21, "Protection system reliability and testability," of Appendix A, "General Design Criteria for Nuclear Power Plants," to 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," requires, among other things, that protection systems be designed for high functional reliability commensurate with the safety function to be performed. Criterion III, "Design Control," of Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," of 10 CFR Part 50 requires, among other things, that quality standards be specified and that design control measures be provided for verifying or checking the adequacy of design.

This guide describes a method acceptable to the NRC staff for complying with the Commission's regulations for promoting high functional reliability for safety-related systems using programmable digital computer systems in nuclear power plants ~~generating stations~~. This method is applicable to designing software, implementing software, and validating computer systems.

For purposes of this guide, structures, systems and components are "safety-related" if they are necessary to ensure (1) the integrity of the reactor coolant pressure boundary, (2) the capability to shut down the reactor and maintain it in a safe shutdown condition, or (3) the capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposures comparable to the guideline exposures of 10 CFR 100.

Any guidance in this document related to information collection activities has been cleared under OMB Clearance No. 3150-0011.

delete per conversation to RC.

B. DISCUSSION

In 1978, a joint working group consisting of members of the American Nuclear Society (ANS) and of the Institute of Electrical and Electronics Engineers (IEEE) was formed with a charter to develop a joint standard containing general guidance for system design and specific guidance on stage-by-stage

testing, overall performance assurance, and documentation of software for -related programmable digital computer systems in safety systems of nuclear power plants. ~~generating stations.~~ Because of the unique nature of programmable digital computer systems, especially with respect to software, the standard was intended to supplement IEEE Std 603-1980, "Standard Criteria for Safety Systems for Nuclear Power Generating Stations,"* which establishes the functional and design criteria for the power, control, and instrumentation portion related of safety systems for nuclear power ~~generating stations~~ plants. This joint standard (designated in draft form as IEEE P 742/ANS 4.3.2) was approved by the IEEE Nuclear Power Engineering Committee and the ANS Nuclear Power Plant Standards Committee and has been published as ANSI/IEEE-ANS-7-4.3.2-1982, "Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations."**

As noted in the Foreword, ANSI/IEEE-ANS 7-4.3.2-1982 will provide, for the present, a basis for reviewing current applications of digital computers in safety-related systems. It is recognized that further effort will be needed with (1) increased industry experience in using programmable digital computers for nuclear power plants, and (2) the advancement in digital computer system technology. The ANSI/IEEE-ANS standard identified the following areas for future work: (a) quantitative software standards, (b) computer security, (c) self testing, (d) distributed computer systems, (e) techniques for independent verification, (f) firmware, and (g) "simplification" objectives. NRC has also recognized this need and has contracted with EGSG-Idaho to undertake such an effort. NRC will consider the results of this study, the experience gained during the NRC review of applications for operating licneses, and any additional pertinent ANSI/IEEE/ANS standards in a future revision of this guide.

delete

C. REGULATORY POSITION

The requirements set forth in ANSI/IEEE-ANS-7-4.3.2-1982 establish a method acceptable to the NRC staff for designing software, verifying software, implementing software, and validating computer systems used in safety -related systems of nuclear power plants ~~generating stations, subject to the following~~. *This endorsement does not include other*

*Copies are available from the Institute of Electrical and Electronics Engineers, 345 East 47th Street, New York, N.Y. 10017.

**Copies are available from the American Nuclear Society, 555 North Kensington Avenue, La Grange Park, Ill. 60525, and the Institute of Electrical and Electronics Engineers, 345 East 47th Street, New York, N.Y. 10017.

standards referenced in ANSI/IEEE-ANS-7-4.3.2-1982. With regard to those referenced standards which are relevant to regulatory actions, the specific applicability or acceptability has been or may be covered separately in other regulatory guides.

~~1. This guide applies to the command, logic, and conditioning elements (but not the sensor and mechanical actuation devices) of safety systems using programmable digital computers.~~

~~2. Section 3.0, "Scope," and Section 3.1, "Hardware Requirements," of ANSI/IEEE-ANS-7-4.3.2-1982 refer to IEEE Std 603-1980. A regulatory guide that will endorse IEEE Std 603-1980 is being developed (IC 600-5, "Criteria for Electric, Instrumentation, and Control Portions of Safety Systems").~~

D. IMPLEMENTATION

The purpose of this section is to provide information to applicants and licensees regarding the NRC staff's plans for using this regulatory guide.

~~This proposed guide has been released to encourage public participation in its development.~~ Except in those cases in which an applicant or licensee proposes an acceptable alternative method for complying with specified portions of the Commission's regulations, the method ~~to be~~ described in ~~the active~~ *this* guide ~~reflecting public comments~~ will be used by the NRC staff in its evaluation of software used in programmable digital computers ~~in safety systems of nuclear generating stations after the implementation date to be specified in the active guide. Implementation by the staff will in no case be earlier than November 1, 1982.~~ *used in safety-related systems of nuclear power plants for all construction permit applications issued after (issue date of guide). Licensees and applicants may use this guide in discussions with the staff as justification for (1) operating license applications currently pending, and (2) modifications to operating licenses.*

VALUE/IMPACT STATEMENT

1. Background

As compared to current analog methods of processing variables, digital computers are considered to offer advantages in accuracy, reliability, and versatility. Merit is seen in their application to safety-related variables and processes.

General guidance for the design of protection systems hardware is provided in IEEE Std 603-1980, "Standard Criteria for Safety Systems for Nuclear Power Generating Stations". Heretofore there has been no such guidance for the design of protection system software. However, a joint working group consisting of members of the American Nuclear Society and of the Institute of Electrical and Electronics Engineers has developed a standard containing general guidance for system design and specific guidance on stage-by-stage testing, overall performance assurance, and documentation of software for programmable digital computer systems in safety-related systems of nuclear power plants. This action endorses the guidance developed by the joint working group.

2. Value/Impact Assessment

rewritten 11-15-84

2.1 General

This regulatory guide endorses the guidance of ANSI/IEEE-ANS-7-4.3.2-1982, "Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations".

2.1.1 Value

The standard embraced by this regulations guide represents an industry concensus on methods to assure the accuracy and reliability of Programmable Digital Computer Systems as applied to safety-related systems.

It provides a standardized approach so that industry and the NRC staff may have a common understanding on software verification and validation procedures, thus minimizing relevant engineering costs for industry and review costs for the staff. Also, errors detected during the design phase through the verification process will, from a cost point of view, be orders of magnitude less expensive than if they are not detected until the operation phase.

2.1.2 Impact

There should be no impact beyond the positive indications in the value statement. It is the only regulation which specifically addresses software development. The guidance was developed through the national concensus standards process jointly by ANS and IEE and was accepted by ANSI. It will become part of the regulations when embraced by this regulatory guide and thus will provide a documented method. It is believed by the staff that plants currently in the licensing process which utilized programmable digital computers for safety-related function have been reviewed in a manner consistent with this proposed regulatory guide. The review of current and future submittals will benefit from this documentation.