U.S. NUCLEAR REGULATORY COMMISSION

November 1985

REGULATORY GUIDE

OFFICE OF NUCLEAR REGULATORY RESEARCH

REGULATORY GUIDE 1.152
(Task IC 127-5)

CRITERIA FOR PROGRAMMABLE DIGITAL COMPUTER SYSTEM SOFTWARE IN SAFETY-RELATED SYSTEMS OF NUCLEAR POWER PLANTS

A. INTRODUCTION

Criterion 21, "Protection system reliability and testability," of Appendix A, "General Design Criteria for Nuclear Power Plants," in 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 the operation of nuclear power plants. This method is applicable to designing software, verifying software, implementing software, and validating computer systems.

Structures, systems, and components are "safety related" if they are relied upon to remain functional during and following design basis events 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 condition, or (3) 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.

The Advisory Committee on Reactor Safeguards has been consulted concerning this guide and has concurred in the regulatory position.

Any information collection activities mentioned in this regulatory guide are contained as requirements in 10 CFR Part 50, which provides the regulatory basis for this guide. The information collection requirements in 10 CFR Part 50 have been cleared under OMB Clearance No. 3150-0011.

B. DISCUSSION

Computer technology can provide new capabilities to nuclear power plant protection and control systems. The NRC staff encourages the application of advanced technology such as programmable digital computers in the operation of nuclear power plants if such advanced technology serves to enhance safety.

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 programmable digital computer systems in safety-related systems of nuclear power plants. 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,"[1] which establishes the functional and design criteria for the power, control, and instrumentation portion of safety-related systems for nuclear power plants. This joint standard 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."[2]

[1] Copies are available from the Institute of Electrical and Electronics Engineers, 345 East 47th Street, New York, NY 10017.

[2] Copies are available from the American Nuclear Society, 555 North Kensington Avenue, La Grange Park, IL 60525, and the Institute of Electrical and Electronics Engineers, 345 East 47th Street, New York, NY 10017.

USNRC REGULATORY GUIDES

Regulatory Guides are issued to describe and make available to the public methods acceptable to the NRC staff of implementing specific parts of the Commission's regulations, to delineate techniques used by the staff in evaluating specific problems or postulated accidents, or to provide guidance to applicants. Regulatory Guides are not substitutes for regulations, and compliance with them is not required. Methods and solutions different from those set out in the guides will be acceptable if they provide a basis for the findings requisite to the issuance or continuance of a permit or license by the Commission.

This guide was issued after consideration of comments received from the public. Comments and suggestions for improvements in these guides are encouraged at all times, and guides will be revised, as appropriate, to accommodate comments and to reflect new information or experience.

Written comments may be submitted to the Rules and Procedures Branch, DRR, ADM, U.S. Nuclear Regulatory Commission, Washington, DC 20555.

The guides are issued in the following ten broad divisions:

1. Power Reactors
2. Research and Test Reactors
3. Fuels and Materials Facilities
4. Environmental and Siting
5. Materials and Plant Protection
6. Products
7. Transportation
8. Occupational Health
9. Antitrust and Financial Review
10. General

Copies of issued guides may be purchased at the current Government Printing Office price. A subscription service for future guides in specific divisions is available through the Government Printing Office. Information on the subscription service and current GPO prices may be obtained by writing the Superintendent of Documents, U.S. Government Printing Office, Post Office Box 37082, Washington, DC 20013-7082.

It should be noted that the standard does not address any follow-on activities such as testing and validation of computer systems beyond the design, implementation, and integration phases. As with any other safety system, there is legitimate concern that measures be provided to ensure that computer systems will continue to perform as designed throughout the life of the plant. Assurance of continued performance is normally accomplished for other safety-related systems by periodic testing. The requirements for periodic testing of hardware and software (revalidation) are contained in the technical specifications. Additional guidance on periodic testing has been provided in Regulatory Guide 1.118, "Periodic Testing of Electric Power and Protection Systems."

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. Although ANSI/IEEE-ANS-7-4.3.2-1982 references IEEE Std 603-1980, ANSI/ASME NQA-1-1979, and IEEE Std 467-1980, these referenced standards are not endorsed by this regulatory guide. They do, however, contain valuable information. If the referenced standards are used, they should be used in a manner consistent w current regulations, which include but are not limited IEEE Std 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations,"[1] and Appendix B of 10 CFR Part 50.

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.

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 described in this guide will be used by the staff in its evaluation of software for all applications in which programmable digital computers are used in safety-related systems of nuclear power plants submitted after November 1985. Licensees and applicants may use this guide as justification of currently pending applications for use of programmable digital computers; however, the staff does not intend to apply this guide to applications currently under review or to operating plants.

VALUE/IMPACT STATEMENT

1. BACKGROUND

Compared to current analog methods of processing variables, digital computers are considered to offer advantages in accuracy, reliability, and versatility, even though they are more vulnerable to subtle failure modes and unauthorized manipulation. Merit is seen in their application to safety-related variables and processes.

General guidance for the design of protection system 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 the Institute of Electrical and Electronics Engineers has developed a standard, ANSI/IEEE-ANS-7-4.3.2-1982, that contains 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 is to endorse the standard developed by the joint working group.

2. VALUE/IMPACT ASSESSMENT

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 endorsed by this regulatory guide represents national consensus on methods to ensure the accuracy and reliability, but not necessarily the security, of programmable digital computer system software as applied to safety-related systems. The security aspects of such systems will be treated on a case-by-case basis during the review process.

This guide 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 NRC staff. Also, errors detected during the design phase through the verification process will be far less expensive than if they were not detected until the operation phase.

2.1.2 Impact

There should be no impact beyond the positive indications in the value statement. This is the only regulatory guide that specifically addresses software development. The guidance was developed through the national consensus standards process jointly by ANS and IEEE and was accepted by ANSI.

It is believed that plants currently in the licensing process that utilize programmable digital computers for safety-related functions have been reviewed in a manner consistent with this regulatory guide. The review of current and future submittals will benefit from this documentation.

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

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300