U.S. NUCLEAR REGULATORY COMMISSION

December 1985

REGULATORY GUIDE

OFFICE OF NUCLEAR REGULATORY RESEARCH

REGULATORY GUIDE 1.153
(Task IC 609-5)

CRITERIA FOR POWER, INSTRUMENTATION, AND CONTROL PORTIONS OF SAFETY SYSTEMS

A. INTRODUCTION

Appendix A, "General Design Criteria for Nuclear Power Plants," to 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," contains, among other things, requirements for the design, reliability, qualification, and testability of the protection system, systems that accomplish safety functions, and other systems (known as auxiliary supporting features) that are essential to the operation of the protection system and the accomplishment of the safety functions. These systems, taken collectively, have been designated as safety systems by the Institute of Electrical and Electronics Engineers (IEEE) and constitute the safety systems addressed in this regulatory guide. The following General Design Criteria are applicable to the power, instrumentation, and control portions of safety systems:

- Criterion 2, "Design Bases for Protection Against Natural Phenomena," requires systems important to safety to be designed to withstand the effects of natural phenomena without loss of capability to perform their safety functions.

- Criterion 4, "Environmental and Missile Design Bases," requires systems important to safety to be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents.

- Criterion 10, "Reactor Design," requires protection systems to be designed with margins to assure that fuel design limits are not exceeded.

- Criterion 12, "Suppression of Reactor Power Oscillations," requires protection systems to be designed to prevent or detect and suppress power oscillations that can result in conditions exceeding fuel design limits.

- Criterion 13, "Instrumentation and Control," requires that instrumentation be provided to monitor variables and systems over their anticipated ranges for normal operation, anticipated operational occurrences, and accidents to assure adequate safety and requires appropriate controls to maintain variables and systems within prescribed operating ranges.

- Criterion 15, "Reactor Coolant System Design," requires that the reactor coolant system and associated auxiliary, control, and protection systems be designed with sufficient margin to assure that the design conditions of the reactor coolant pressure boundary are not exceeded during any condition of normal operation, including anticipated operational occurrences.

- Criterion 17, "Electric Power Systems," requires electric power systems to be provided to permit functioning of structures, systems, and components important to safety.

- Criterion 18, "Inspection and Testing of Electric Power Systems," requires electric power systems important to safety to be designed to permit periodic inspection and testing of such systems for operability and functional performance.

- Criterion 20, "Protection System Functions," requires a protection system to sense anticipated operational occurrences and accidents and initiate operation of appropriate systems to assure that acceptable limits are not exceeded.

- Criterion 21, "Protection System Reliability and Testability," requires the protection system to be designed with high functional reliability and inservice testability. This criterion also requires redundancy and independence to provide protection against single failures and retention of redundancy (except where justified) in the event equipment is removed for service. On-line testing is required.

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. Information on current GPO prices may be obtained by contacting the Superintendent of Documents, U.S. Government Printing Office, Post Office Box 37082, Washington, DC 20013-7082, telephone (202)275-2060 or (202)275-2171.

• Criterion 22, "Protection System Independence," requires that the effects of natural phenomena, normal operation, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protective function.

• Criterion 23, "Protection System Failure Modes," requires that the protection system be designed to fail into a safe state or into a state demonstrated to be acceptable on some other basis if conditions such as disconnection of the system, loss of energy, or postulated adverse environments are experienced.

• Criterion 24, "Separation of Protection and Control Systems," requires separation of protection and control systems to the extent that failure or removal from service of control equipment or equipment common to protection and control leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system and requires that safety not be impaired as a result of the interconnection of protection and control systems.

• Criterion 25, "Protection System Requirements for Reactivity Control Malfunctions," requires that the protection system be designed to assure that specified acceptable fuel design limits will not be exceeded for any single malfunction of the reactivity control systems.

• Criterion 29, "Protection Against Anticipated Operational Occurrences," requires that protection systems and reactivity control systems be designed to be highly reliable in accomplishing their safety functions in the event of anticipated operational occurrences.

• Criteria 34, "Residual Heat Removal," 35, "Emergency Core Cooling," 38, "Containment Heat Removal," 41, "Containment Atmosphere Cleanup," and 44, "Cooling Water," require suitable redundancy, interconnections, and isolation capabilities to assure that, for onsite and for offsite electric power system operation, the safety function can be accomplished.

• Criteria 37, "Testing of Emergency Core Cooling System," 40, "Testing of Containment Heat Removal System," 43, "Testing of Containment Atmosphere Cleanup Systems," and 46, "Testing of Cooling Water System," require designs to permit periodic functional testing of these systems, the operability and performance of the active components of the system, and the operability of each of these systems as a whole, including the full operational sequence that brings each system into operation.

• Criterion 54, "Piping Systems Penetrating Containment," requires redundancy, reliability, and performance that reflect the importance of the isolation systems to safety. Capability for periodic testing is also required.

In addition, § 50.55a, "Codes and Standards," of 10 CFR Part 50 requires in paragraph (h) that protection systems meet the requirements set forth in IEEE Std 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations"* (also designated ANSI N42.7-1972).

Section 50.49, "Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants," of 10 CFR Part 50 requires that a program be established for qualifying safety-related electric equipment and certain non-safety-related electric and post-accident monitoring equipment.

This guide describes a method acceptable to the NRC staff for complying with the Commission's regulations with respect to the design, reliability, qualification, and testability of the power, instrumentation, and control portions of safety-related systems. This guide applies to all types of nuclear plants.

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

IEEE Std 603-1980, "Criteria for Safety Systems for Nuclear Power Generating Stations,"* was prepared by Subcommittee 6, Safety-Related Systems, of the IEEE Nuclear Power Engineering Committee (NPEC). IEEE Std 603-1980 was approved by NPEC on November 15, 1979, and by the IEEE Standards Board on March 13, 1980.

The requirements and recommendations of IEEE Std 603-1980 on the power, instrumentation, and control portions of safety systems incorporate the requirements and recommendations contained in IEEE Std 279-1971, which is limited to protection systems only. Compliance with the provisions of IEEE Std 603-1980, as supplemented in Section C of this guide, is considered by the NRC staff to satisfy the provisions of IEEE Std 279-1971. (The converse is not true owing to the larger scope of IEEE Std 603-1980.)

The specific equipment to be used in implementing the requirements of IEEE Std 603-1980 is outside the scope of the standard. However, the NRC staff encourages the application of advanced technology such as programmable digital computers in the operation of nuclear power plants if such technology serves to enhance safety.

*Copies are available from the Institute of Electrical and Electronics Engineers Service Center, 445 Hoes Lane, Piscataway, NJ 08854.

With respect to Paragraph 1.2, "Application," of IEEE Std 603-1980, in the context of NRC classification, the fire protection system is not classified as a safety-related system. Additionally, in applying the criteria of the standard, it is helpful to understand that the following are considered to be synonymous: (1) electric portions of the safety system, (2) Class 1E equipment, and (3) safety-related electric equipment as defined in § 50.49 of 10 CFR Part 50. It should also be noted that the scope of the standard is broader than (1), (2), and (3) above since, for example, pneumatic instruments may be part of the safety system.

The following is a brief discussion of the basis of each regulatory position:

1. The terms "safety system" and "safety-related system" have evolved separately, and it is essential in applying IEEE Std 603-1980 that the relationship of the terms (as stated in Regulatory Position 1) be understood.

2. IEEE Std 497-1977 is referenced in IEEE Std 603-1980, but some of the requirements of IEEE Std 497-1977 are at variance with current regulatory practice. Hence, in Regulatory Position 2, reference to IEEE Std 497-1977 in IEEE Std 603-1980 is being replaced with reference to Regulatory Guide 1.97, "Instrumentation for Light-Water-Cooled Nuclear Power Plants To Assess Plant and Environs Conditions During and Following an Accident," which provides specific recommendations for the identification, design, installation, and maintenance of certain instrumentation considered Type A in Regulatory Guide 1.97.

3. In Regulatory Position 3, Section 6.3.1(1) of IEEE Std 603-1980 has been changed to correct a printing error in the standard.

4. Figure 7 of IEEE Std 603-1980, which provides an interpretation of Section 6.3.1, is confusing and could be misleading in that the upper left "diamond" cannot accommodate an event that, by itself, results in a condition requiring a safety function while simultaneously causing action by a non-safety system. A modified chart is included as Figure 1 of this guide as stated in Regulatory Position 4.

5. Additional IEEE standards that are referenced in other sections of the standard are listed in Section 3 of IEEE Std 603-1980. Because the NRC staff may not have endorsed these other standards, a caution regarding their use is provided in Regulatory Position 5.

C. REGULATORY POSITION

The requirements contained in IEEE Std 603-1980 provide a method acceptable to the NRC staff for complying with the Commission's regulations with regard to the design, reliability, qualification, and testability of the power,* instrumentation, and control portions of safety systems as modified and supplemented by the following:

1. The term "safety system" used throughout IEEE Std 603-1980 should be understood to be synonymous with "safety-related system," in which the term "safety-related" has the meaning stated in § 50.49(b)(1) of 10 CFR Part 50.

2. For displays for manually controlled actions covered in Section 5.8.1 of IEEE Std 603-1980, the provisions for Type A instruments in Regulatory Guide 1.97, "Instrumentation for Light-Water-Cooled Nuclear Power Plants To Assess Plant and Environs Conditions During and Following an Accident," should be followed instead of IEEE Std 497-1977.

3. Instead of the first sentence in Section 6.3.1(1) of IEEE Std 603-1980, the first sentence in Section 4.7.4.1 of IEEE Std 279 should be used: "Alternate channels, not subject to failure resulting from the same single event, shall be provided to limit the consequences of this event to a value specified by the design bases."

4. Section 6.3.1 of IEEE Std 603-1980 references Figure 7, a decision chart for applying the requirements of the section. Figure 1 of this guide should be used in lieu of Figure 7 of IEEE Std 603-1980.

5. Section 3 of IEEE Std 603-1980 lists additional standards that are referenced in the standard. Those referenced standards not endorsed by a regulatory guide or incorporated into the regulations contain valuable information; if used, they should be used in a manner consistent with current regulatory practice.

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 NRC staff in its evaluation of the design, reliability, qualification, and testability of the power, instrumentation, and control portions of safety-related systems for construction permit applications docketed after November 1985. All other applications will be evaluated against the provisions of this guide only to the extent that the licensee elects to use the guide as a basis for system modifications requiring staff approval.

*The term power includes electric, pneumatic, and hydraulic power.

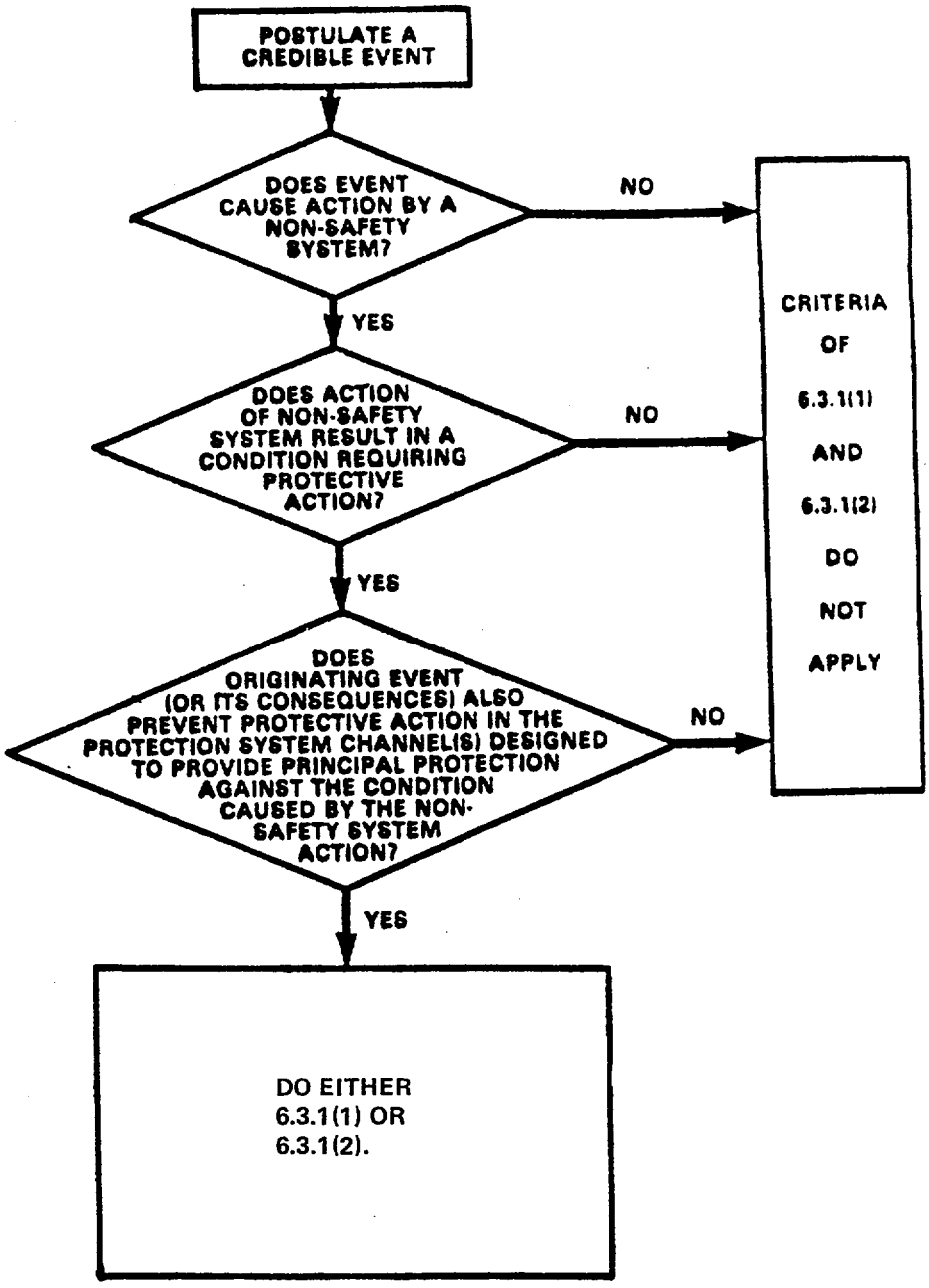

FIGURE 1. Replacement for Figure 7 of IEEE Std 603-1980

VALUE/IMPACT STATEMENT

1. BACKGROUND

The licensee of a nuclear power plant is required by the Commission's regulations to provide for the design, reliability, qualification, and testability of the protection systems, systems that perform protection functions, and other systems that are essential to the operation of protection systems and the accomplishment of the protection functions. IEEE Std 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations," is incorporated into the regulations and provides requirements and recommendations for the protection systems. IEEE Std 603-1980, "Criteria for Safety Systems for Nuclear Power Generating Stations," provides the same criteria as IEEE Std 279-1971 for protection systems, but it is expanded in scope and provides additional guidance by including criteria for protection system actuation functions and auxiliary systems. This regulatory guide endorses IEEE Std 603-1980 with appropriate supplements.

2. VALUE/IMPACT ASSESSMENT

2.1 General

The guidance in IEEE Std 603-1980 for the design, reliability, qualification, and testability of the power, instrumentation, and control portions of safety-related systems is endorsed by this regulatory guide.

2.1.1 Value

This action should result in more effective design, reliability, qualification, and testability of safety-related systems, including auxiliary supporting features. The guide establishes the NRC position on a national consensus standard and therefore reduces uncertainty as to what the staff considers acceptable.

2.1.2 Impact

There should be no impact. IEEE Std 603 was developed with the intent that it would eventually supersede IEEE Std 279. Its scope includes the protection system as covered in IEEE Std 279, and it is further expanded to include power sources and actuation functions as well as protection systems. No new requirements are imposed with the expansion in scope. This expansion in scope is essentially covered by guidance provided in existing regulatory guides. For instance, Regulatory Guide 1.32, "Criteria for Safety-Related Electric Power Systems for Nuclear Power Plants," endorses IEEE Std 308, which provides similar guidance for power sources. Regulatory Guide 1.53, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems," endorses IEEE Std 379 and provides similar guidance for meeting the single-failure criterion. Regulatory Guide 1.75, "Physical Independence of Electric Systems," endorses IEEE Std 384 and provides similar guidance for physical independence of redundant systems and equipment.

2.2 Definitions

Regulatory Position 1 was included to show the relationship of the term "safety system" and the term "safety-related" as it pertains to systems, thus clarifying the term used in the standard.

2.2.1 Value

The relationship should be clarified to eliminate the possibility of misunderstanding.

2.2.2 Impact

There is no impact since no new requirements are imposed.

2.3 Information Displays

Regulatory Position 2 was included to replace the guidance of IEEE Std 497-1977 with that of Regulatory Guide 1.97 as it pertains to display for manually controlled actions.

2.3.1 Value

Regulatory Guide 1.97 was developed to provide the staff's position on display for manually controlled actions. The acceptability of all of the guidance of IEEE Std 497-1977 has not yet been determined by the staff—some of its provisions are at variance with staff recommendations, i.e., some ways of meeting the single-failure criterion.

2.3.2 Impact

There is no impact since no new requirements are imposed.

2.4 Interaction

Regulatory Position 3 was included to correct a printing error.

2.4.1 Value

The error should be corrected to enable proper understanding of the standard.

2.4.2 Impact

There is no impact since no new requirements are imposed.

2.5 Interaction Chart

Regulatory Position 4 was included to replace a figure that was confusing. The figure addresses the decision process for applying the requirements of Section 6.3.1 of IEEE Std 603-1980.

2.5.1 Value

The new figure eliminates the confusion that was in the original figure and will aid the decision-making process.

2.5.2 Impact

There is no impact as the new chart was supplied by the group who authored IEEE Std 603-1980, and it imposes no new requirements.

2.6 References

Regulatory Position 5 was included to provide the staff position on the referenced national consensus standards in IEEE Std 603-1980.

2.6.1 Value

Regulatory Position 5 provides the user of the standard with the NRC staff position on using the standards listed as references.

2.6.2 Impact

There is no impact since no new requirements are imposed.

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

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300

FIRST CLASS MAIL
POSTAGE & FEES PAID
USNRC
WASH. D.C.
PERMIT No. G-67