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

May 2002
Division 1
Draft DG-1118

DRAFT REGULATORY GUIDE

Contact: S.K. Aggarwal (301)415-6005

DRAFT REGULATORY GUIDE DG-1118

(Proposed Revision 1 of Regulatory Guide 1.53)

APPLICATION OF THE SINGLE-FAILURE CRITERION TO SAFETY SYSTEMS

A. INTRODUCTION

Section 50.55a, "Codes and Standards," of 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," requires in 10 CFR 50.55a(h) that the protection systems meet the requirements set forth in the Institute of Electrical and Electronics Engineers (IEEE) Criteria for Nuclear Power Plant Protection Systems (IEEE Std 279) or that the safety systems must meet the requirements set forth in IEEE Std 603-1991, "Criteria for Safety Systems for Nuclear Power Generating Stations." Section 4.2 of IEEE Std 279-1971[*] states that any single failure within the protection system will not prevent proper protective action at the system level when required. Section 5.1 of IEEE Std 603-1991* states that the safety system must perform all safety functions required for a design basis event in the presence of (a) any single detectable failure within the safety systems concurrent with all identifiable but nondetectable failures, (b) all failures caused by the single failure, and (c) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions.

This regulatory guide describes a method acceptable to the NRC staff for complying with the Commission's regulations with respect to satisfying the single-failure criterion.

Regulatory guides are issued to describe methods acceptable to the NRC staff for implementing specific parts of the NRC's regulations, to explain techniques used by the staff in evaluating specific problems or postulated accidents, and to provide guidance to applicants. Regulatory guides are not substitutes for regulations, and compliance with regulatory guides is not required. Regulatory guides are not substitutes for regulations, and compliance with regulatory guides is not required. Regulatory guides

[*] Copies may be purchased from the Institute of Electrical and Electronics Engineers, Inc., 445 Hoes Lane, Piscataway, NJ 08855-1331.

are issued in draft form for public comment to involve the public in developing the regulatory positions. Draft regulatory guides have not received complete staff review; they therefore do not represent official NRC staff positions at this time.

Comments are specifically invited on the second paragraph under Section B, "Discussion," of this proposed Revision 1 of Regulatory Guide 1.53.

The information collections contained in this draft regulatory guide are covered by the requirements of 10 CFR Part 50, which were approved by the Office of Management and Budget (OMB), approval number 3150-3011. The NRC may not conduct or sponsor, and a person is not required to respond to, a request for information or an information collection requirement unless the requesting document displays a currently valid OMB control number.

B. DISCUSSION

IEEE Std 379-2000, "Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," was prepared by Working Group SC 6.3 of IEEE Nuclear Power Engineering Committee and was approved by the IEEE Standards Board on September 21, 2000. The standard provides guidance on the application of the single-failure criterion to the electrical power, instrumentation, and control portions of nuclear power plant safety systems. The systems include the actuation and protection systems, as well as the sense, command, and execute features of the power system. The guidance in this standard has been developed for electrical systems. However, where the interface with mechanical systems is unavoidable (e.g., sensing lines), the mechanical portions are considered to be part of the electrical system with which they interface.

The safety systems must perform all required safety functions for a design basis event in the presence of the following: (1) Any single detectable failure within the safety systems concurrent with all identifiable but nondetectable failures, (2) all failures caused by the single failures, (3) all failures and spurious system actions that cause, or are caused by, the design basis event that requires the safety function. The single failure could occur prior to, or at any time during, the design basis event for which the safety system is required to function.

C. REGULATORY POSITION

Conformance with the requirements of IEEE Std 379-2000, "Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," provides a method acceptable to the NRC staff for satisfying the NRC's regulations with respect to the application of the single-failure criterion to the electrical power, instrumentation, and control portions of nuclear power plant safety systems.

Section 2 of IEEE Std 379-2000 references several industry codes and standards. If a referenced standard has been separately incorporated into the NRC's regulations, licensees and applicants must comply with the standard as set forth in the regulation. If the referenced standard has been endorsed by the NRC staff in a regulatory guide, the standard constitutes an acceptable method of meeting a regulatory requirement as described in the regulatory guide. If a referenced standard has been neither incorporated into the NRC's regulations nor endorsed in a regulatory guide, licensees and applicants may consider and use the information in the referenced standard, if appropriately justified, consistent with 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 guide. No backfitting is intended or approved in connection with the issuance of this guide.

This proposed revision has been released to encourage public participation in its development. Except in those cases in which an applicant or licensee proposes or has previously established an acceptable alternative method for complying with specified portions of the NRC's regulations, the method to be described in the final guide (reflecting public comments) will be used in the evaluation of submittals in connection with applications for construction permits, design certifications, operating licenses, and combined licenses. Licensees of operating nuclear power plants will have the option to use for safety system modifications (1) the June 1973 issue of Regulatory Guide 1.53 (which endorses IEEE Std. 379-1972 with exceptions) and be subjected to review by the staff on a case-by-case basis or (2) this Revision 1 that endorses IEEE Std. 379-2000 with no exceptions.

REGULATORY ANALYSIS

BACKGROUND

The safety systems must, with precision and reliability, maintain plant parameters within acceptable limits established for each design basis event. The power, instrumentation, and control portions of each safety system consist of more than one safety group, any one of which can accomplish the safety function. Thus, the safety systems must perform all safety functions required for a design basis event in the presence of any single detectable failure within the safety systems. This is the single-failure criterion.

1. PROBLEM

In June 1973, Regulatory Guide 1.53, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems," was issued to describe acceptable methods for complying with the NRC's regulations for meeting the single-failure criterion. This was accomplished by the conditional endorsement of IEEE Std 379-1972, "IEEE Trial-Use Guide for the Application of the Single-Failure Criterion to Nuclear Power Generating Station Protection Systems." When Regulatory Guide 1.53 was issued, the NRC staff had planned to update the guide after the expiration of the trial period of IEEE Std 379-1972. However, the NRC staff has never updated Regulatory Guide 1.53 as previously planned.

Since the issuance of Regulatory Guide 1.53, IEEE Std 379-1972 has been revised and published as a new edition in 1977, 1988, 1994, and 2000. The nuclear power plant licensees have been using various editions of IEEE Std 379 when making modifications to their plants. Therefore, the guidance in Regulatory Guide 1.53 has become outdated.

Instrumentation and control (I&C) systems that use digital computers in safety systems make extensive use of advanced technology, i.e., equipment and design practices that are expected to be significantly and functionally different from current designs. These designs include, but are not limited to, the use of microprocessors, digital systems and displays, fiber optics, multiplexing, and different isolation techniques to achieve needed independence and redundancy. For the past several years, the NRC staff has encouraged the application of digital computers in the design and operation of nuclear power plants. In the early 1970s, when IEEE Std 379-1972 was issued, this technology was not used in nuclear power plants and, therefore, the 1972 version did not provide any guidance for application of a single-failure criterion to digital computers. Guidance was added to IEEE Std 379-2000 to address single-failure analysis in designs that use digital computers.

2. OBJECTIVE

The objective of the regulatory action is to update NRC guidance on application of the single-failure criterion to safety systems.

3. TECHNICAL APPROACH

There have been numerous changes to IEEE Std 379 since the initial issuance of this standard in 1972. The scope of the standard was expanded from the "protection system" to the

"safety system," consistent with the scope of IEEE Std. 603-1991, "Criteria for Safety Systems for Nuclear Power Generating Stations." The methodology used to perform a single-failure analysis has been refined and additional guidance has been added. In addition, there have been numerous format and administrative changes. The following is a summary of the significant changes.

(1) The scope of the standard was expanded from the protection system to the complete safety system. The new scope is congruent with the scope of IEEE Std 603-1991. This change is also consistent with 10 CFR 50.55a(h).

(2) A concise "Statement of the Single-Failure" was added.

(3) Additional guidance was added to address single-failure analysis in designs that use digital computers.

(4) Guidance was added on the application of the single-failure criterion to shared systems.

(5) The procedure for a single-failure analysis was clarified and strengthened. This procedure is more rigorous than that contained in IEEE Std 379-1972. In addition, an unnecessary process step that classified single failures into four types was deleted.

(6) Guidance was added on the use of a probabilistic assessment to determine whether certain failures and events can be excluded from a single-failure analysis.

(7) Guidance was added concerning the need to include the instrument sensing lines in the single-failure analysis.

(8) Important information previously contained in the appendices was incorporated into the body of IEEE Std 379-2000.

(9) Most of the information previously in Appendix B was either moved to a more appropriate location in IEEE Std 384, "Criteria for Independence of Class 1E Equipment and Circuits," or deleted because it is now contained in the fire protection rule.

(10) Additional references and definitions were added to IEEE Std 379 as a result of the evolution in the higher-level standard from IEEE Std 279-1971 to IEEE Std 603-1991.

(11) Administrative changes resulted in a reformatting of IEEE Std 379-2000. The following table shows the mapping of requirements from the 1972 version to the 2000 version of IEEE Std 379.

IEEE Std 379-1972 Section Number	IEEE Std 379-2000 Section Number
3(1)	5.1
3(2)	5.2
3(3)	5.2
3(4)	5.3
3(5)	6.1(1) through 6.1(4)
3(6)	5.4
3(7)	6.3.3
5.1	4
5.2	5.2
5.3	5.5
6.1	6.1
6.2	6.2.1
6.3	6.2.2
6.4	6.2.3
6.5	5.5
6.6	6.3 through 6.6 and 6.3.1

IEEE Std 379-2000 addresses the regulatory positions and issues identified in the June 1973 issue of Regulatory Guide 1.53. The staff has worked with IEEE in developing IEEE Std 379-2000, and all three original exceptions have been satisfactorily resolved. A discussion of the original regulatory positions and issues is included in the “Introduction” section of IEEE Std 379-2000.

Thus, IEEE 379-2000 is a much improved national consensus standard and it reflects the current state of technology.

4. CONCLUSION

It is recommended that the NRC revise Regulatory Guide 1.53, since this action should enhance the licensing process. The staff has concluded that the proposed action will reduce unnecessary burden on both the NRC and its licensees, and it will result in an improved process for the design and evaluation of the single-failure criterion to safety systems. Furthermore, the staff sees no adverse effects associated with revising Regulatory Guide 1.53. Use of this revision is optional by licensees of the currently operating nuclear power plants.

BACKFIT ANALYSIS

The regulatory guide does not require a backfit analysis as described in 10 CFR 50.109 (c) because the use of this revision of Regulatory Guide 1.53 is voluntary by the licensees of currently operating nuclear power plants.