



REGULATORY GUIDE

OFFICE OF NUCLEAR REGULATORY RESEARCH

REGULATORY GUIDE 1.53

(Draft was issued as DG-1118)

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 protection systems for plants with construction permits issued after January 1, 1971, but before May 13, 1999, must meet the requirements stated in either IEEE Std. 279, "Criteria for Protection Systems for Nuclear Power Generating Stations,"¹ or IEEE Std. 603-1991, "Criteria for Safety Systems for Nuclear Power Generating Stations."¹ For nuclear power plants with construction permits issued before January 1, 1971, protection systems must be consistent with their licensing basis or may meet the requirements of IEEE Std 603-1991. The safety systems for plants with construction permits issued after May 13, 1999, must meet the requirements of IEEE Std. 603-1991.

IEEE Std. 279-1971 states that a "protection system" encompasses all electric and mechanical devices and circuitry (from sensors to actuation device input terminals) involved in generating those signals associated with the protective function. These signals include those that actuate a reactor trip and that, in the event of a serious reactor accident, actuate engineered safety features (ESFs), such as containment isolation, core spray, safety injection, pressure reduction, and air cleaning. "Protective function" is defined in IEEE Std. 279-1971 as "the sensing of one or more variables associated with a

¹ Copies may be purchased from the Institute of Electrical and Electronics Engineers, Inc., 445 Hoes Lane, Piscataway, NJ 08855.

Regulatory guides are issued to describe and make available to the public such information as methods acceptable to the NRC staff for implementing specific parts of the NRC's regulations, techniques used by the staff in evaluating specific problems or postulated accidents, and data needed by the NRC staff in its review of applications for permits and licenses. 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 Directives Branch, ADM, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001.

Regulatory guides are issued in 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; and 10, General.

Single copies of regulatory guides (which may be reproduced) may be obtained free of charge by writing the Distribution Services Section, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, or by fax to (301)415-2289, or by email to DISTRIBUTION@NRC.GOV. Electronic copies of this guide and other recently issued guides are available at NRC's home page at WWW.NRC.GOV through the Electronic Reading Room, Accession Number ML033220006.

particular generating station condition, signal processing, and the initiation and completion of the protective action at values of the variables established in the design bases.”

IEEE Std. 603-1991 uses the term “safety systems” rather than “protection systems” to define its scope. A “safety system” is defined in IEEE Std. 603-1991 as “a system that is relied upon to remain functional during and following design basis events to ensure: (i) the integrity of the reactor coolant pressure boundary, (ii) the capability to shut down the reactor and maintain it in a safe shutdown condition, or (iii) 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.” A “safety function” is defined in IEEE Std. 603-1991 as “one of the processes or conditions (for example, emergency negative reactivity insertion, post-accident heat removal, emergency core cooling, post-accident radioactivity removal, and containment isolation) essential to maintain plant parameters within acceptable limits established for a design basis event.”

Section 4.2 of IEEE Std 279-1971¹ 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 603-1991¹ 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. 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.

The information collections contained in this 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 3150-0011. 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,”¹ 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 a part of the electrical system with which they interface.

The NRC recognizes that “protection systems” are a subset of “safety systems.” Safety system is a broad-based and all-encompassing term, embracing the protection system in addition

to other electrical systems. This regulatory guide is not intended to change the scope of the systems covered in the final safety analysis report for the currently operating nuclear power plants. Therefore, the regulatory guidance in this revision applies only to plant protection systems for currently operating nuclear power plants; and any application to a broader scope, namely safety system modifications, is voluntary. The staff continues to encourage, but not require, operating nuclear power plants to comply with IEEE Std. 603-1991 and IEEE Std. 379-2000 for future system-level modifications.

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 methods 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.

Except when an applicant or licensee proposes or has previously established an acceptable alternative method for complying with specified portions of the NRC’s regulations, the methods described in this guide will be used in the evaluation of submittals in connection with applications for construction permits, design certifications, operating licenses, and combined licenses for application of the single-failure criterion to safety systems. It will also be used to evaluate submittals from operating reactor licensees who voluntarily propose to initiate protection system (or safety system) modifications if there is a clear nexus between the proposed modifications and this guidance for applying the single-failure criterion.

REGULATORY ANALYSIS

A separate Regulatory Analysis was not prepared for this Revision 2 of Regulatory Guide 1.53. The Regulatory Analysis that was prepared for and printed with the draft of this guide, DG-1118, in May 2002 is still applicable. Copies of DG-1118, with the Regulatory Analysis, are available in the NRC's Electronic Reading Room through ADAMS, accession number ML021160080. Copies are also available for inspection or copying for a fee from the NRC Public Document Room at 11555 Rockville Pike (first floor), Rockville, MD; the PDR's mailing address is USNRC PDR, Washington, DC 20555; telephone 301-415-4737 or 800-397-4209; fax 301-415-3548; email PDR@NRC.GOV.