



REGULATORY GUIDE

OFFICE OF NUCLEAR REGULATORY RESEARCH

REGULATORY GUIDE 1.170

(Draft was DG-1056)

SOFTWARE TEST DOCUMENTATION FOR DIGITAL COMPUTER SOFTWARE USED IN SAFETY SYSTEMS OF NUCLEAR POWER PLANTS

A. INTRODUCTION

In 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," paragraph 55a(a)(1) requires, in part, that systems and components be designed, tested, and inspected to quality standards commensurate with the safety function to be performed.¹ Criterion 1, "Quality Standards and Records," of Appendix A, "General Design Criteria for Nuclear Power Plants," to 10 CFR Part 50 requires, in part, that a quality assurance program be established and implemented in order to provide adequate assurance that systems and components important to safety will satisfactorily perform their safety functions.¹ Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," to 10 CFR Part 50 describes criteria that must be met by a quality assurance program for systems and components that prevent or mitigate the consequences of postulated accidents. In particular, besides the systems and components that directly prevent or mitigate the consequences of postulated accidents, the criteria of Appendix B also apply to all activities affecting the safety-related functions of such systems and components, such as designing, purchasing, installing, testing, operating, maintaining, or

modifying. A specific requirement is contained in 10 CFR 50.55a(h), which requires that reactor protection systems satisfy the criteria of IEEE Std 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations."² Paragraph 4.3 of IEEE Std 279³ states that quality of components is to be achieved through the specification of requirements known to promote high quality, such as requirements for design, inspection, and test.

Many of the criteria in Appendix B to 10 CFR Part 50 contain requirements closely related to the activities of verification and testing.¹ Criterion I, "Organization," requires the establishment and execution of a quality assurance program. Criterion II, "Quality Assurance Program," requires the quality assurance program to take into account the need for verification of quality by inspections and tests. Criterion III, "Design Control," requires, in part, that measures be established for verifying and checking the adequacy of design, such as by the performance of a suitable testing program, and

¹In this regulatory guide, many of the regulations have been paraphrased; see 10 CFR Part 50 for the full text.

²Revision 1 of Regulatory Guide 1.153, "Criteria for Safety Systems," endorses IEEE Std 603-1991, "Criteria for Safety Systems for Nuclear Power Generating Stations," as a method acceptable to the NRC staff for satisfying the NRC's regulations with respect to the design, reliability, qualification, and testability of the power, instrumentation, and control portions of the safety systems of nuclear power plants.

³IEEE publications may be obtained from the IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854.

USNRC REGULATORY GUIDES

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 Commission'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 Review and Directives Branch, DFIPS, ADM, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001.

The guides are issued in the following ten broad divisions:

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

Single copies of regulatory guides may be obtained free of charge by writing the Printing, Graphics and Distribution Branch, Office of Administration, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001; or by fax at (301)415-5272.

Issued guides may also be purchased from the National Technical Information Service on a standing order basis. Details on this service may be obtained by writing NTIS, 5285 Port Royal Road, Springfield, VA 22161.

that design control measures be applied to items such as the delineation of acceptance criteria for inspections and tests. Criterion V, "Instructions, Procedures, and Drawings," requires activities affecting quality to be prescribed by documented instructions, procedures, or drawings of a type appropriate to the circumstances and that these activities be accomplished in accordance with these instructions, procedures, or drawings. Criterion V further requires that instructions, procedures, and drawings include appropriate quantitative or qualitative acceptance criteria for determining that important activities have been satisfactorily accomplished. Criterion XI, "Test Control," requires establishment of a test program to ensure that all testing required to demonstrate that structures, systems, and components will perform satisfactorily in service is identified and performed in accordance with written test procedures that incorporate the requirements and acceptance limits contained in applicable design documents. Test procedures must include provisions for ensuring that all prerequisites for the given test have been met, that adequate test instrumentation is available and used, and that the test is performed under suitable environmental conditions. Criterion XI also requires that test results be documented and evaluated to ensure that test requirements have been satisfied. Finally, Criteria VI, "Document Control," and XVII, "Quality Assurance Records," provide for the control of the issuance of documents, including changes thereto, that prescribe all activities affecting quality and provide for the maintenance of sufficient records to furnish evidence of activities affecting quality. The latter requires test records to identify the inspector or data recorder, the type of observation, the results, the acceptability of the results, and the action taken in connection with any deficiencies noted.

This regulatory guide endorses ANSI/IEEE Std 829-1983, "IEEE Standard for Software Test Documentation,"³ with the exceptions stated in the Regulatory Position. This guide describes methods acceptable to the NRC staff for complying with parts of the NRC's regulations for achieving high functional reliability and design quality in software used in safety systems.⁴ In particular, the methods are consistent with the previously cited General Design Criteria and the criteria for quality assurance programs of Appendix B as they apply to the documentation of software testing activi-

⁴The term "safety systems" is synonymous with "safety-related systems." The General Design Criteria cover systems, structures, and components "important to safety." The scope of this regulatory guide is, however, limited to "safety systems," which are a subset of "systems important to safety."

ties. The criteria of Appendices A and B apply to systems and related quality assurance processes, and if those systems include software, the requirements extend to the software elements.

In general, information provided by regulatory guides is reflected in the Standard Review Plan (NUREG-0800). The Office of Nuclear Reactor Regulation uses the Standard Review Plan to review applications to construct and operate nuclear power plants. This regulatory guide will apply to the revised Chapter 7 of the Standard Review Plan.

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, approval number 3150-0011. The NRC may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number.

B. DISCUSSION

The use of industry consensus standards is part of an overall approach to meeting the requirements of 10 CFR Part 50 when developing safety systems for nuclear power plants. Compliance with standards does not guarantee that regulatory requirements will be met. However, compliance does ensure that practices accepted within various technical communities will be incorporated into the development and quality assurance processes used to design safety systems. These practices are based on past experience and represent industry consensus on approaches used for development of such systems.

Software incorporated into instrumentation and control systems covered by Appendix B will be referred to in this regulatory guide as safety system software. For safety system software, software testing is an important part of the effort to achieve compliance with the NRC's requirements. Software engineering practices rely, in part, on software testing to meet general quality and reliability requirements consistent with Criteria 1 and 21 of Appendix A to 10 CFR Part 50, as well as Criteria I, II, III, V, VI, XI, and XVII in Appendix B.

Current practice for the development of software for high-integrity applications includes the use of a software life cycle process that incorporates software testing activities. See IEEE Std 1074-1991, "IEEE Standard for Developing Software Life Cycle Processes."³ Software testing is a key element in software verification and validation activities, as indicated by IEEE Std 1012-1986, "IEEE Standard for Software Verification and Validation Plans,"³ and IEEE Std

7-4.3.2-1993, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations."³ The latter is endorsed by Revision 1 of Regulatory Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants." The consensus standard, ANSI/IEEE Std 829-1983, "IEEE Standard for Software Test Documentation" (reaffirmed in 1991), defines software test documentation and specifies its form and content. The term 'documentation' is used here in accordance with the first meaning given in IEEE Std 610.12-1990, "IEEE Standard Glossary of Software Engineering Terminology," which defines documentation as a collection of documents on a given subject. IEEE Std 829-1983 describes a method for software test documentation consistent with the previously cited regulatory requirements as they apply to safety system software.

The documentation identified in IEEE Std 829-1983 falls into three categories: test planning, test specification, and test reporting. All three categories provide for test information consistent with the requirements of Appendix B to 10 CFR Part 50, in particular, with the requirements of Criterion XI, "Test Control," as applied to software. The test planning category consists of a test plan that addresses key aspects of the test program, such as scope, risks, tasks, resources, responsibilities, and acceptance (pass or fail) criteria for the software item being tested. The test specification category consists of test designs, test cases, and test procedures that contain the detailed procedures and instructions for testing as well as the feature or test case acceptance criteria to be employed during the testing effort. This category is particularly relevant to Criterion V, "Instructions, Procedures, and Drawings." The test reporting category consists of transmittal reports, test incident reports, test logs, and test summary reports that provide for the recording and summarization of test events and that serve as the basis for evaluating test results. All information in this category is summarized in the test summary report. This category addresses the requirements of parts of Criterion VI, "Document Control," Criterion XI, "Test Control," and Criterion XVII, "Quality Assurance Records," as applied to software. The documentation in the test reporting category contains most of the specific information itemized in Criterion XVII (although anomaly resolution typically will be handled through the change process of the software configuration management (SCM) function). IEEE Std 829-1983 also provides for the inclusion of additional material in any of its defined documentation; therefore, any special testing information associated with unique circumstances may also be included.

C. REGULATORY POSITION

The requirements contained in IEEE Std 829-1983, "IEEE Standard for Software Test Documentation," provide an approach acceptable to the NRC staff for meeting the requirements of 10 CFR Part 50 as they apply to the test documentation of safety system software subject to the exceptions listed below. The appendices to this standard are not covered by this regulatory guide. (In this Regulatory Position, the cited criteria are in Appendix B to 10 CFR Part 50 unless otherwise noted.)

To meet the requirements of 10 CFR 50.55a(h) and Appendix A to 10 CFR Part 50 as assured by complying with the criteria of Appendix B applied to the test documentation of safety system software, the following exceptions are necessary and will be considered by the NRC staff in the review of submittals from applicants and licensees.

1. TEST PROGRAM

Criterion XI, "Test Control," requires that a test program be established to ensure that all testing required to demonstrate that systems and components will perform satisfactorily in service is identified and performed in accordance with written test procedures that incorporate requirements and acceptance limits contained in applicable design documents. Criterion I, "Organization," Criterion II, "Quality Assurance Program," Criterion III, "Design Control," Criterion V, "Instructions, Procedures, and Drawings," Criterion VI, "Document Control," and Criterion XVII, "Quality Assurance Records," contain requirements regarding information associated with testing. IEEE Std 829-1983 does not mandate the use of all of its software test documentation in any given test phase. It directs the user to specify the documents required for a particular test phase. If a subset of the IEEE Std 829-1983 documentation is chosen for a particular test phase, information necessary to meet regulatory requirements regarding software test documentation must not be omitted. As a minimum, this information includes:

- Qualifications, duties, responsibilities, and skills required of persons and organizations assigned to testing activities,
- Environmental conditions and special controls, equipment, tools, and instrumentation needed for accomplishing the testing,
- Test instructions and procedures incorporating the requirements and acceptance limits in applicable design documents,

- Test prerequisites and the criteria for meeting them,
- Test items and the approach taken by the testing program,
- Test logs, test data, and test results,
- Acceptance criteria, and
- Test records indicating the identity of the tester, the type of observation, the results and acceptability, and the action taken in connection with any deficiencies.

Any of the above information items that are not present in the subset selected for a particular test phase must be incorporated into the appropriate documentation as an additional item.

2. SOFTWARE DOCUMENTATION

Criterion VI, "Document Control," and Criterion XVII, "Quality Assurance Records," as well as 10 CFR 21.51, "Maintenance and Inspection of Records," of 10 CFR Part 21, "Reporting of Defects and Noncompliance," require the control and retention of documents and records affecting quality. Since design control measures must be applied to acceptance criteria for tests and since some software test documentation is reused and evolves during the course of software development and software maintenance (for example, regression test documentation), such test documentation should be controlled as one or more configuration items under a software configuration management system. Test records, such as test reports, must be maintained as quality records and should be controlled by the software configuration management system.

3. TEST DOCUMENTATION

IEEE Std 829-1983 describes software test documentation as a set of individual documents. It is acceptable for the individual documents to be incorporated into larger test documents, provided the identity of each component document is retained.

4. SYSTEM TESTING

Criterion XI, "Test Control," requires that testing demonstrate that systems and components will perform satisfactorily in service. In section 4.2.2 of IEEE Std 829-1983, in describing the features to be tested by a given test design, it is noted that other features may be exercised but not identified. Each feature in safety system software is to be formally tested under at least one test design.

5. TRACEABILITY

Criterion XI, "Test Control," requires that testing demonstrate that systems and components will perform satisfactorily in service. Traceability analyses, relating functions and test cases, provide a means for ensuring that all functions are tested. These analyses are addressed in planning for software verification and validation.⁵ In section 5.2.2, IEEE Std 829-1983 suggests consideration of supplying references to item documentation as part of test case documentation. These references must be included in the test case documentation unless equivalent traceability information is maintained elsewhere in the verification and validation records.

6. OTHER CODES AND STANDARDS

Standards endorsed by regulatory guides sometimes refer to other standards. These references to other standards should be treated individually. If a referenced standard has been incorporated separately into the NRC's regulations, licensees and applicants must comply with that standard as set forth in the regulation. If the referenced standard has been endorsed in a regulatory guide, the standard constitutes a method acceptable to the NRC staff 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 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. No backfitting is intended or approved in connection with this guide.

Except in those cases in which an applicant proposes an acceptable alternative method for complying with the 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 and operating licenses. This guide will also be used to evaluate submittals from operating reactor licensees that propose system modifications voluntarily initiated by the licensee if there is a clear nexus between the proposed modifications and this guidance.

⁵See IEEE Std 1012-1986, "IEEE Standard for Software Verification and Validation Plans."

BIBLIOGRAPHY

Hecht, H., A.T. Tai, K.S. Tso, "Class 1E Digital Systems Studies," NUREG/CR-6113, USNRC, October 1993.¹

Institute of Electrical and Electronics Engineers, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," IEEE Std 7-4.3.2, 1993.

Lawrence, J.D., "Software Reliability and Safety in Nuclear Reactor Protection Systems," NUREG/CR-6101 (UCRL-ID-117524, Lawrence Livermore National Laboratory), USNRC, November 1993.¹

Lawrence, J.D., and G.G. Preckshot, "Design Factors for Safety-Critical Software," NUREG/CR-6294, USNRC, December 1994.¹

Seth, S., et al., "High Integrity Software for Nuclear Power Plants: Candidate Guidelines, Technical Basis and Research Needs," NUREG/CR-6263, USNRC, June 1995.¹

USNRC, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," Regulatory Guide 1.152, Revision 1, January 1996.²

USNRC, "Standard Review Plan," NUREG-0800, February 1984.

¹Copies may be purchased at current rates from the U.S. Government Printing Office, P.O. Box 37082, Washington, DC 20402-9328 (telephone (202)512-2249); or from the National Technical Information Service by writing NTIS at 5285 Port Royal Road, Springfield, VA 22161. Copies are available for inspection or copying for a fee from the NRC Public Document Room at 2120 L Street NW., Washington, DC; the PDR's mailing address is Mail Stop LL-6, Washington, DC 20555-0001; telephone (202)634-3273; fax (202)634-3343.

²Single copies of regulatory guides may be obtained free of charge by writing the Office of Administration, Printing, Graphics and Distribution Branch, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001; or by fax at (301)415-5272. Copies are available for inspection or copying for a fee from the NRC Public Document Room at 2120 L Street NW, Washington, DC; the PDR's mailing address is Mail Stop LL-6, Washington, DC 20555-0001; telephone (202)634-3273; fax (202)634-3343.

REGULATORY ANALYSIS

A separate regulatory analysis was not prepared for this regulatory guide. The regulatory analysis prepared for Draft Regulatory Guide DG-1056, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," provides the regulatory basis for this guide. A copy of the regulatory analysis is available for inspection and copying for a fee at the NRC Public Document Room, 2120 L Street NW., Washington, DC; the PDR's mailing address is Mail Stop LL-6, Washington, DC 20555-0001; phone (202)634-3273; fax (202)634-3343.



Federal Recycling Program

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, DC 20555-0001

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, \$300

FIRST CLASS MAIL
POSTAGE AND FEES PAID
USNRC
PERMIT NO. G-67