



REGULATORY GUIDE

OFFICE OF NUCLEAR REGULATORY RESEARCH

REGULATORY GUIDE 1.171

(Draft was DG-1057)

SOFTWARE UNIT TESTING 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,¹ that systems and components be designed, tested, and inspected to quality standards commensurate with the safety function to be performed. Criterion 1, "Quality Standards and Records," of Appendix A, "General Design Criteria for Nuclear Power Plants," to 10 CFR Part 50 requires, in part,¹ 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. Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," to 10 CFR Part 50 describes criteria that a quality assurance program for systems and components that prevent or mitigate the consequences of postulated accidents must meet. 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 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 279-1971³ 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 testing activities. Criterion I, "Organization," requires the establishment and execution of a quality assurance program. Criterion II, "Quality Assurance Program," requires, in part, that the program take into account the need for special controls, processes, test equipment, tools, and skills to attain the required quality, as well as the need for verification of quality by inspection and test. 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

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, DFPS, 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)415-6272.

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.

suitable testing program, and 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 assure 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 1008-1987, "IEEE Standard for Software Unit Testing,"³ with the exceptions stated in the Regulatory Position. IEEE Std 1008-1987 describes a method acceptable to the NRC staff for complying with parts of the NRC's regulations for promoting high functional reliability and design quality in software used in safety systems.⁴ In particular, the method is consistent with the previously cited General Design Criteria and the criteria for quality assurance programs of Appendix B as they apply to software unit testing. The criteria of Appendices A and B apply to systems and related quali-

ty 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 that document.

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 of Appendix B.

The consensus standard, IEEE Std 1008-1987 (reaffirmed in 1993), defines a method for planning, preparing for, conducting, and evaluating software unit testing. The method described is consistent with the previously cited regulatory requirements as they apply to safety system software.

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, e.g., IEEE Std 1074-1991, "IEEE Standard for Developing Software Life Cycle

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."

Processes.”³ Software testing, including software unit 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.” A common approach to software testing [NUREG/CR-6101, “Software Reliability and Safety in Nuclear Reactor Protection Systems” (November 1993); NUREG/CR-6263, “High Integrity Software for Nuclear Power Plants: Candidate Guidelines, Technical Basis and Research Needs” (June 1995)]⁵ utilizes a three-level test program to help ensure quality in a complex software product or complex set of cooperating software products, i.e., unit-level testing, integration-level testing, and system-level testing such as system validation tests or acceptance tests. IEEE Std 1008-1987 delineates an approach to the unit testing of software that is based on the assumption of a larger context established by verification and validation (V&V) planning as well as general planning for the full range of testing activities to be applied. Therefore, software unit testing performed in accordance with IEEE Std 1008-1987 should be consistent with planning information established in V&V plans and higher-level software test plans, although that planning information is not within the scope of IEEE Std 1008-1987.

C. REGULATORY POSITION

The requirements in ANSI/IEEE Std 1008-1987, “IEEE Standard for Software Unit Testing,” provide an approach acceptable to the NRC staff for meeting the requirements of 10 CFR Part 50 as they apply to the unit testing of safety system software, subject to the provisions listed below. The appendices to IEEE Std 1008-1987 are not endorsed by this regulatory guide except as noted below. Appendix A to this standard provides guidance regarding the implementation of the software unit testing approach, and Appendix B to the standard provides context regarding software engineering information and testing assumptions that underlie the software unit testing approach.

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 to 10 CFR Part 50 ap-

plied to the unit testing of safety system software, the following exceptions are necessary and will be considered by the NRC staff in the review of submittals from licensees and applicants. (In this section, the cited criteria are in Appendix B to 10 CFR Part 50 unless otherwise noted.)

1. SOFTWARE TESTING DOCUMENTATION

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 bearing on information associated with testing. IEEE Std 1008-1987, in section 1.1, mandates the use of the Test Design Specification and the Test Summary Report defined by ANSI/IEEE Std 829-1983, “IEEE Standard for Software Test Documentation.” In addition, IEEE Std 1008-1987 either incorporates additional information into these two documents or indicates the need for additional documents. Regardless of whether these two documentation formats are used, the documentation used to support software unit testing (either documentation used directly in the software unit testing activity or documentation of the overall testing effort) must include information necessary to meet regulatory requirements as applied to software test documentation. 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 the accomplishment of 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,

⁵Copies are available 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.

- 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 documentation selected to support software unit testing must be incorporated as additional items.

2. TEST PROGRAM

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. The two aspects of test coverage that are particularly important for the unit testing of safety system software are coverage of requirements and coverage of the internal structure of the code.

2.1 Coverage of Requirements

For safety system software, those requirements identified as essential to the safety determination⁶ must be tested. Section 3.2.2(5) of IEEE Std 1008-1987 suggests consideration of expected use of the unit in the determination of features to be tested. All features and associated procedures, states, state transitions, and associated data characteristics essential to the safety determination must be included in the testing.

2.2 Coverage of Internal Structure

Section 3.1.2(2) of IEEE Std 1008-1987 specifies statement coverage (covering each source language statement with a test case) as a criterion for measuring the completeness of the software unit testing activity. Statement coverage is a very weak criterion for measuring test completeness [See Beizer⁷ and NUREG/CR-6263⁸]. Therefore, the staff does not endorse statement coverage as a sufficient coverage criterion for software unit testing. For safety system software, the unit test coverage criteria to be employed should be identified and justified.

⁶Regulatory Guide 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," endorses IEEE Std 830-1993, "IEEE Recommended Practice for Software Requirements Specifications."

⁷Boris Beizer, *Software Testing Techniques*, Van Nostrand Reinhold, 1990.

⁸S. Seth et al., "High Integrity Software for Nuclear Power Plants: Candidate Guidelines, Technical Basis and Research Needs," NUREG/CR-6263, June 1995.

3. TEST PROGRAM RECORDS

Criteria VI, "Document Control," and XVII, "Quality Assurance Records," as well as 10 CFR 21.51, require the control and retention of documents and records affecting quality. In addition, Criterion III, "Design Control," requires that design changes be subject to design control measures commensurate with those applied to the original design. Preservation of testing products is discussed in section 3.8.2(4) of IEEE Std 1008-1987. Since design control measures must be applied to acceptance criteria for tests and since some software testing materials are frequently re-used and evolve during the course of software development and software maintenance (for example, regression test materials), such materials should be configuration items under change control of a software configuration management system.⁹ Additional information on this topic is provided in section A6 of Appendix A to IEEE Std 1008-1987.

4. INDEPENDENCE IN SOFTWARE VERIFICATION

Criterion III, "Design Control," imposes an independence requirement for the verification and checking of the adequacy of the design, requiring that those persons who verify and check be different from those who accomplish the design. Therefore, independence is an additional requirement for software unit testing. Either those persons who establish the requirements-based elements for a software unit test must be different from those who designed or coded the software, or there must be independent review of the establishment of the requirements-based elements. The guidance in section A7 of Appendix A to IEEE Std 1008-1987 provides acceptable ways to meet this requirement for software unit testing. These independent persons must be sufficiently competent in software engineering to ensure that software unit testing is adequately implemented.

5. OTHER STANDARDS

Section 1.3 of IEEE Std 1008-1987 references ANSI/IEEE Std 729-1983, "IEEE Standard Glossary of Software Engineering Terminology," and ANSI/IEEE Std 829-1983, "IEEE Standard for Software Test Documentation." These referenced 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

⁹Regulatory Guide 1.169 endorses IEEE Std 828-1990, "IEEE Standard for Software Configuration Management Plans," and IEEE Std 1042-1987, "IEEE Guide to Software Configuration Management," to provide guidance for general software configuration management plans and their implementation.

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 backfit-

ting is intended or approved in connection with the issuance of this proposed 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.

BIBLIOGRAPHY

Beizer, Boris, *Software Testing Techniques*, Van Nostrand Reinhold, 1990.

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, 1993.¹

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

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.

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 1984.¹

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-1057, "Software Unit Testing 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