DRAFT REGULATORY GUIDE

Contact: K. Sturzebecher
(301) 251-7494

DRAFT REGULATORY GUIDE DG-1208
(Proposed Revision 1 of Regulatory Guide 1.171, dated September 1997)

SOFTWARE UNIT TESTING FOR DIGITAL COMPUTER SOFTWARE USED IN SAFETY SYSTEMS OF NUCLEAR POWER PLANTS

A. INTRODUCTION

This guide describes a method that the staff of the U.S. Nuclear Regulatory Commission (NRC) considers acceptable for use in complying with NRC regulations with respect to the software unit testing of digital computer software used in the safety systems of nuclear power plants.

The regulatory framework that the NRC has established for nuclear power plants consists of a number of regulations and supporting guidelines applicable to the software unit testing of digital computer software. Title 10, of the *Code of Federal Regulations*, Part 50, "Domestic Licensing of Production and Utilization Facilities" (10 CFR Part 50) (Ref. 1), Appendix A, "General Design Criteria for Nuclear Power Plants," General Design Criterion (GDC) 1, "Quality Standards and Records," requires, in part, that quality standards be established and implemented to provide adequate assurance that systems and components important to safety will satisfactorily perform their safety functions. GDC 21, "Protection System Reliability and Testability," requires, in part, that the protection system be designed for high functional reliability. 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, in addition to the systems and components that directly prevent or mitigate the consequences of postulated accidents, Appendix B criteria also apply to all activities, including design, purchasing, installation, testing, operation, maintenance, or modification, that affect the safety-related functions of such systems and components.

In 10 CFR 50.55a(a)(1) requires, in part, that systems and components be designed, fabricated, erected, tested, and inspected to quality standards commensurate with the safety function to be performed. The regulation in 10 CFR 50.55a(h) requires that reactor protection systems satisfy the criteria in Institute

---

of Electrical and Electronics Engineers (IEEE) Standard (Std.) 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," including a correction sheet dated January 30, 1995 (Ref. 2), or in IEEE Std. 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations" (Ref. 3). These criteria shall be part of the evaluation of the recognized quality codes and standards selected for their applicability, adequacy, and sufficiency and shall be supplemented or modified as needed to assure a quality product and that it will perform the required safety function. The guidance on the safety systems equipment employing digital computers, and programs or firmware requires quality standards be used for testing software units.

This regulatory guide endorses American National Standards Institute (ANSI)/IEEE Std. 1008-1987, "IEEE Standard for Software Unit Testing" (Ref. 4), with the exceptions stated in the regulatory positions. ANSI/IEEE Std. 1008-1987, which was reaffirmed in 2002, describes a method acceptable to the NRC staff for complying with NRC regulations for promoting high functional reliability and design quality in the software used in safety systems.[1] In particular, the method is consistent with the previously cited GDC in Appendix A to 10 CFR Part 50 and the criteria for quality assurance programs in Appendix B to 10 CFR Part 50 as they apply to software unit testing. The criteria in Appendices A and B apply to systems and related quality assurance processes, and the requirements extend to the software elements if those systems include software.

The NRC issues regulatory guides to describe to the public methods that the staff considers acceptable for use in implementing specific parts of the agency's regulations, to explain techniques that the staff uses in evaluating specific problems or postulated accidents, and to provide guidance to applicants. However regulatory guides are not substitutes for regulations and compliance with them is not required. The information provided by this regulatory guide is also in the Standard Review Plan, NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," Chapter 7, "Instrumentation and Controls," (Ref. 5). The NRC staff uses the NRC Standard Review Plan to review 10 CFR Part 50 and 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants," (Ref. 6) license applications.

This regulatory guide contains information collection requirements covered by 10 CFR Part 50 that the Office of Management and Budget (OMB) approved under OMB control number 3150-0011. The NRC may neither conduct nor sponsor, and a person is not required to respond to, an information collection request or requirement unless the requesting document displays a currently valid OMB control number. This regulatory guide is a rule as designated in the Congressional Review Act (5 U.S.C. 801–808). However, OMB has not found it to be a major rule as designated in the Congressional Review Act.

B. DISCUSSION

Background

The use of industry consensus standards, such as IEEE standards, is part of an overall approach to meet the requirements of 10 CFR Part 50 when developing safety systems for nuclear power plants. Compliance with these 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

---

[1]   The term "safety systems" is synonymous with "safety-related systems." The scope of the GDC includes systems, structures, and components "important to safety." However, the scope of this regulatory guide is limited to "safety systems," which are a subset of "systems important to safety."

based on past experience and represent industry consensus on approaches used for the development of such systems.

This regulatory guide refers to software incorporated into the instrumentation and control systems covered by Appendix B to 10 CFR Part 50 as "safety system software." For safety system software, software testing is an important part of the effort to comply with NRC regulations. Software engineering practices rely, in part, on software testing to meet general quality and reliability requirements consistent with GDC 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.

Several criteria in Appendix B to 10 CFR Part 50 contain requirements closely related to testing activities. These listed Criterions are only part of and not the entire requirement:

- Criterion I, "Organization," requires, in part, 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 (1) special controls, processes, test equipment, tools, and skills necessary to attain the required quality and (2) the verification of quality through inspections and tests.

- Criterion III, "Design Control," requires, in part, that measures be established for verifying and checking the adequacy of the design (e.g., through the performance of a 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, in part, activities affecting quality 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 VI, "Document Control," requires, in part, that all documents that prescribe activities affecting quality, such as instructions, procedures, and drawings, be subject to controls that ensure that documents, including changes, are reviewed for adequacy and approved for release by authorized personnel.

- Criterion XI, "Test Control," requires, in part, establishment of a test program to assure 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.

- Criterion XVII, "Quality Assurance Records," requires, in part, that sufficient records be maintained so that data that are closely associated with the qualifications of personnel, procedures, and equipment are identifiable and retrievable. Test records must identify the inspector or data recorder, the type of observation made, the results, the acceptability of the results, and the action taken in connection with any noted deficiencies.

Description of Change

Both the original version of this regulatory guide and this revision endorse ANSI/IEEE Std. 1008-1987. Subsequently, associated software regulatory guides various related software standards have been developed or updated and this revision of Regulatory Guide 1.171 is being updated to be consistent with these standards and related guidance. The applicant or licensee should consider the hierarchy guidance of these different regulatory guides and standards that relate to the software development process and unit testing. For example, Regulatory Guide 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Ref. 7), endorses IEEE Std. 829-2008, "IEEE Standard for Software and System Test Documentation" (Ref. 8), and provides an approach that the NRC staff considers acceptable for meeting the requirements of 10 CFR Part 50 as they apply to the test documentation, including unit test documentation, of safety system software. The endorsed consensus standard, ANSI/IEEE Std. 1008-1987, defines a method for planning, preparing, conducting, and evaluating software unit testing that is consistent with the previously cited regulatory requirements as they apply to safety system software.

Related Guidance

Current practice for the development of software for safety-related applications includes the use of a software life-cycle process that incorporates software testing activities (e.g., IEEE Std. 1074-2006, "IEEE Standard for Developing a Software Life Cycle Process" (Ref. 9), as endorsed by Regulatory Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Ref. 10)). Software testing, including software unit testing, is a key element in software verification and validation (V&V) activities, as indicated by IEEE Std. 1012-2004, "IEEE Standard for Software Verification and Validation" (Ref. 11), and IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations" (Ref. 12). Software testing consists of several levels. NUREG/CR-6101, "Software Reliability and Safety in Nuclear Reactor Protection Systems," issued November 1993 (Ref. 13), and NUREG/CR-6263, "High Integrity Software for Nuclear Power Plants: Candidate Guidelines, Technical Basis, and Research Needs," issued June 1995 (Ref. 14), provide a common approach to software testing. This approach includes a three-level test program to help ensure quality in a complex software product or a 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). ANSI/IEEE Std. 1008-1987 delineates an approach to the unit testing of software that assumes a larger context established by V&V planning and general planning for the application of the full range of testing activities. This context may be defined, for example, in IEEE Std. 1012-2004, as endorsed by Regulatory Guide 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Ref. 15). Therefore, software unit testing that licensees perform in accordance with ANSI/IEEE Std. 1008-1987 should be consistent with the planning information established in V&V plans and higher level software test plans, although that planning information is not within the scope of ANSI/IEEE Std. 1008-1987.

This regulatory guide is based on standards and describes methods acceptable for any safety system software, and discusses the required V&V activities. The applicant or licensee determines how the required activities will be implemented.

Other Codes and Standards

This regulatory guide endorses the use of one or more voluntary consensus codes or standards developed by external organizations. These codes or standards may contain references to other codes or standards. These references should be considered individually. If a referenced standard has been incorporated separately into NRC 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 for meeting a regulatory requirement as described in the specific regulatory guide. If a referenced standard has been neither incorporated into NRC regulations nor endorsed in a regulatory guide, licensees and applicants may consider and use the information in the referenced standard, if appropriately justified and consistent with current regulatory practice.

Harmonization with International Standards

This regulatory guide endorses, in whole or in part, multiple international consensus standards produced by international organizations such as the Institute of Electrical and Electronic Engineers (IEEE).

The IEEE is a non-profit professional association dedicated to advancing technological innovation and excellence. It has more than 400,000 members in more than 160 countries and produces 30% of the world's literature in the electrical and electronics engineering and computer science fields including multiple tutorials and standards produced by its standardization committees.

Endorsement, in whole or in part, of multiple international standards reduces the need for the development of unique NRC standards and is consistent with the agency goal of improved harmonization with international organizations.

C. STAFF REGULATORY GUIDANCE

The requirements in ANSI/IEEE Std. 1008-1987 provide an acceptable approach for meeting the NRC's regulatory requirements on the unit testing of safety system software with the exceptions and additions listed in these regulatory positions. In this section of the guide, the cited criterion refers to Appendix B to 10 CFR Part 50 unless otherwise noted. This regulatory guide does not endorse the appendices to ANSI/IEEE Std. 1008-1987, except as noted below.

1. Software Testing Documentation

Section 1.1 of ANSI/IEEE Std. 1008-1987 mandates the use of the test design specifications and the test summary report documents, which can be found in IEEE Std. 829-2008, Clauses 10, "Level Test Design" and 17, "Master Test Report", respectively. In addition, ANSI/IEEE Std. 1008-1987 either incorporates additional information into these two documents or indicates the need for additional documentation. Regardless of whether the licensee uses these two documentation formats, its documentation to support software unit testing (either documentation used directly in the software unit testing activity or documentation of the overall testing effort) should include information necessary to meet regulatory requirements as applied to software test documentation. As a minimum, this information should include the following:

a. qualifications, duties, responsibilities, and skills required of persons and organizations assigned to testing activities;

b. special conditions and controls, equipment, tools, and instrumentation needed for the accomplishment of testing;

c. test instructions and procedures that incorporate the requirements and acceptance limits in applicable design documents;

d. test prerequisites and the criteria for meeting these requirements and acceptance limits;

e. test items and the approach taken by the testing program;

f. test logs, test data, and test results;

g. acceptance criteria; and

h. test records that indicate the identity of the tester, the type of observation made, the results and acceptability, and the action taken in connection with any deficiencies.

The licensee should incorporate any information regarding the items listed above that are not in the documentation selected to support software unit testing as additional items.

2. Test Program

The coverage of requirements and the internal structure of the code are two particularly important aspects of test coverage necessary for the unit testing of safety system software, as follows:

a. Coverage of Requirements. The testing should include all features and associated procedures, states, state transitions, and associated data characteristics essential to the safety determination.

b. Coverage of Module Structure. Section 3.1.2(2) of ANSI/IEEE Std. 1008-1987 specifies statement coverage (covering each source language statement with a test case) as a criterion for measuring the completeness of software unit testing. The staff believes that statement coverage is an insufficient criterion for measuring test completeness (Ref. 14 and Ref. 16). Therefore, the staff does not endorse statement coverage as a sufficient criterion for software unit testing. For safety system software, the licensee should identify and justify the unit testing coverage criteria that it will use.

3. Test Program Records

Criteria VI and XVII and 10 CFR 21.51, "Maintenance and Inspection of Records" (Ref. 17), require the control and retention of documents and records that affect quality. In addition, Criterion III requires the licensee to subject design changes to design control measures commensurate with those that it applied to the original design. Section 3.8.2(4) of ANSI/IEEE Std. 1008-1987 discusses the preservation of testing products. Included with the testing products preservation are the test iterations caused by any task, procedure and design criteria variations or deviations from the original IEEE 829-2008, Clauses 8 and 9, "Master Test Plan" and "Level Test Plans." Since the design control measures are required for testing acceptance criteria and because some software testing materials are frequently reused and evolve during the course of software development and software maintenance (e.g., regression test

materials), such materials should be configuration items under the change control of a software configuration management system.

4.   Independence Software Verification

Criterion III imposes an independence requirement for the verification and checking of the adequacy of the design. IEEE Std. 1008-1987 does not include a requirement for independent software verification. The Regulatory Guide 1.168 provides additional guidance on testing independence.

5.   References to ANSI/IEEE Std. 829-1983

ANSI/IEEE Std. 1008-1987 includes references to ANSI/IEEE Std. 829-1983; however, ANSI/IEEE Std. 829-1983 has been revised since the publication of ANSI/IEEE Std.1008-1987. With the new ANSI/IEEE Std. 829-2008 revision there are added levels of test documentation for the licensee and applicant to consider, which also includes unit test documentation. Thus IEEE Std. 829-2008, which is endorsed by Regulatory Guide 1.170, should be used.

6.   Annexes

ANSI/IEEE Std. 1008-1987 contains the following informative appendixes listed below. These appendixes are listed here as sources of information; they have not received regulatory endorsement unless otherwise noted:

- Appendix A, "Implementation and Usage Guidelines," provides some additional guidance on using the standard. Although this is a useful introduction to several topics, the NRC does not endorse the appendix because it does not provide sufficient guidance on how to perform specific activities.

- Appendix B, "Concepts and Assumptions," contains a variety of topics that relate unit testing to software engineering in general and that discuss testing assumptions. This appendix is helpful but out of date; therefore, the NRC does not endorse it.

- Appendix C, "Sources for Techniques and Tools," lists documents that relate to unit testing. This list is out of date; therefore, the NRC does not endorse it.

- Appendix D, "General References," lists a basic set of references on software testing. This list is out of date; therefore, the NRC does not endorse it.

D. IMPLEMENTATION

The purpose of this section is to provide information on how applicants and licensees[2] may use this guide and information regarding the NRC's plans for using this regulatory guide. In addition, it describes how the NRC staff complies with the Backfit Rule (10 CFR 50.109) and any applicable finality provisions in 10 CFR Part 52.

---

[2]   In this section, "licensees" refers to licensees of nuclear power plants under 10 CFR Parts 50 and 52; and the term "applicants," refers to applicants for licenses and permits for (or relating to) nuclear power plants under 10 CFR Parts 50 and 52, and applicants for standard design approvals and standard design certifications under 10 CFR Part 52.

Use by Applicants and Licensees

Applicants and licensees may voluntarily[3] use the guidance in this document to demonstrate compliance with the underlying NRC regulations. Methods or solutions that differ from those described in this regulatory guide may be deemed acceptable if they provide sufficient basis and information for the NRC staff to verify that the proposed alternative demonstrates compliance with the appropriate NRC regulations. Current licensees may continue to use guidance the NRC found acceptable for complying with the identified regulations as long as their current licensing basis remains unchanged.

Licensees may use the information in this regulatory guide for actions which do not require NRC review and approval such as changes to a facility design under 10 CFR 50.59. Licensees may use the information in this regulatory guide or applicable parts to resolve regulatory or inspection issues.

This regulatory guide is not being imposed upon current licensees and may be voluntarily used by existing licensees.

If a licensee believes that the NRC is either using this regulatory guide or requesting or requiring the licensee to implement the methods or processes in this regulatory guide in a manner inconsistent with the discussion in this Implementation section, then the licensee may file a backfit appeal with the NRC in accordance with the guidance in NUREG-1409 and NRC Management Directive 8.4.

Use by NRC Staff

During regulatory discussions on plant specific operational issues, the staff may discuss with licensees various actions consistent with staff positions in this regulatory guide, as one acceptable means of meeting the underlying NRC regulatory requirement. Such discussions would not ordinarily be considered backfitting even if prior versions of this regulatory guide are part of the licensing basis of the facility. However, unless this regulatory guide is part of the licensing basis for a facility, the staff may not represent to the licensee that the licensee's failure to comply with the positions in this regulatory guide constitutes a violation.

If an existing licensee voluntarily seeks a license amendment or change and (1) the NRC staff's consideration of the request involves a regulatory issue directly relevant to this new or revised regulatory guide and (2) the specific subject matter of this regulatory guide is an essential consideration in the staff's determination of the acceptability of the licensee's request, then the staff may request that the licensee either follow the guidance in this regulatory guide or provide an equivalent alternative process that demonstrates compliance with the underlying NRC regulatory requirements. This is not considered backfitting as defined in 10 CFR 50.109(a)(1) or a violation of any of the issue finality provisions in 10 CFR Part 52.

The NRC staff does not intend or approve any imposition or backfitting of the guidance in this regulatory guide. The NRC staff does not expect any existing licensee to use or commit to using the guidance in this regulatory guide, unless the licensee makes a change to its licensing basis. The NRC staff does not expect or plan to request licensees to voluntarily adopt this regulatory guide to resolve a generic regulatory issue. The NRC staff does not expect or plan to initiate NRC regulatory action which would require the use of this regulatory guide. Examples of such unplanned NRC regulatory actions include issuance of an order requiring the use of the regulatory guide, requests for information under 10 CFR 50.54(f) as to whether a licensee intends to commit to use of this regulatory guide, generic

---

[3] In this section, "voluntary" and "voluntarily" means that the licensee is seeking the action of its own accord, without the force of a legally binding requirement or an NRC representation of further licensing or enforcement action.

communication, or promulgation of a rule requiring the use of this regulatory guide without further backfit consideration.

Additionally, an existing applicant may be required to adhere to new rules, orders, or guidance if 10 CFR 50.109(a)(3) applies.

REFERENCES[4]

1. Code of Federal Regulations (CFR), *Title 10, Energy,* Part 50, "Domestic Licensing of Production and Utilization Facilities."

2. Institute of Electrical and Electronic Engineers (IEEE) Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," IEEE, Piscataway, NJ, 1991.[5]

3. IEEE Std. 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations," IEEE, Piscataway, NJ, 1971.

4. IEEE Std. 1008-1987, "IEEE Standard for Software Unit of Testing," IEEE, Piscataway, NJ, 1987.

5. U. S. Nuclear Regulatory Commission (NRC), NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," Chapter 7, "Instrumentation and Controls," NRC, Washington, DC. (http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0800/ch7/)

6. CFR, *Title 10, Energy,* Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants."

7. NRC, Regulatory Guide 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," NRC, Washington, DC.

8. IEEE Std. 829-2008, "IEEE Standard for Software Test Documentation," IEEE, Piscataway, NJ, 2008.

9. IEEE Std. 1074-2006, "IEEE Standard for Developing a Software Life Cycle Process," IEEE, Piscataway, NJ, 2006.

10. NRC, Regulatory Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," NRC, Washington, DC.

11. IEEE Std. 1012-2004, "IEEE Standard for Software Verification and Validation," IEEE, Piscataway, NJ, 2004.

12. IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," IEEE, Piscataway, NJ, 2003.

---

[4] Publicly available NRC published documents are available electronically through the Electronic Reading Room on the NRC's public Web site at: http://www.nrc.gov/reading-rm/doc-collections/. The documents can also be viewed online or printed for a fee in the NRC's Public Document Room (PDR) at 11555 Rockville Pike, Rockville, MD; the mailing address is USNRC PDR, Washington, DC 20555; telephone 301-415-4737 or 800-397-4209; fax 301-415-3548; and e-mail pdr.resource@nrc.gov.

[5] Copies of Institute of Electrical and Electronics Engineers (IEEE) documents may be purchased from the Institute of Electrical and Electronics Engineers Service Center, 445 Hoes Lane, PO Box 1331, Piscataway, NJ 08855, or through the IEEE's public Web site at http://www.ieee.org/publications_standards/index.html.

13. NRC, NUREG/CR-6101, "Software Reliability and Safety in Nuclear Reactor Protection Systems," NRC, Washington, DC, November 1993. (ADAMS Accession No. ML072750055)

14. NRC, NUREG/CR-6263, "High Integrity Software for Nuclear Power Plants: Candidate Guidelines, Technical Basis, and Research Needs," NRC, Washington, DC, June 1995. (ADAMS Accession Nos. ML063470590, ML063600344, and ML063470593)

15. NRC, Regulatory Guide 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," NRC, Washington, DC.

16. Beizer, B., *Software Testing Techniques*, Van Nostrand Reinhold, New York, NY, 1990.[6]

17. CFR, *Title 10, Energy,* Part 21.51, "Maintenance and Inspection of Records"

---

[6] Boris Beizer, *Software Testing Techniques*, June 1990, ISBN-10: 1850328803, ISBN-13: 978-1850328803 can be purchased at many book stores and online locations, including the following Web site: http://www.amazon.com/Software-Testing-Techniques-Boris-Beizer/dp/1850328803/ref=sr_1_1?s=books&ie=UTF8&qid=1288897895&sr=1-1.