U.S. NUCLEAR REGULATORY COMMISSION

September 1997

REGULATORY GUIDE

OFFICE OF NUCLEAR REGULATORY RESEARCH

REGULATORY GUIDE 1.168

(Draft was DG–1054)

VERIFICATION, VALIDATION, REVIEWS, AND AUDITS 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,[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 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 279–1971[3] 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.

In Appendix B,[1] "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," to 10 CFR Part 50, many of the criteria contain requirements closely related to the activities of verification and testing. Criterion I, "Organization," of Appendix B, in describing the establishment and execution of a quality assurance program, specifies that applicants must (a) assure that an appropriate quality assurance program is established and effectively executed and (b)

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

[2]Revision 1 of Regulation 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.

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

verify, such as by checking, auditing, and inspection, that activities affecting safety-related functions have been correctly performed. Criterion II, "Quality Assurance Program," of Appendix B states, in part, that activities affecting quality must be accomplished under suitably controlled conditions. Controlled conditions include the use of appropriate equipment, suitable environmental conditions for accomplishing the activity, and assurance that all prerequisites for the given activity have been satisfied. It also states, in part, that the program must take into account the need for verification of quality by inspection and test. Criterion III, "Design Control," of Appendix B requires, in part, that design control measures provide for verifying or checking the adequacy of design. Criterion XI, "Test Control," requires, in part, that a test program be established 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. Finally, Criterion XVIII, "Audits," requires, in part, that a comprehensive system of planned and periodic audits be carried out to verify compliance with all aspects of the quality assurance program and to determine the effectiveness of the program.

This regulatory guide endorses IEEE Std 1012–1986,[3] "IEEE Standard for Software Verification and Validation Plans," and IEEE Std 1028–1988,[3] "IEEE Standard for Software Reviews and Audits." IEEE Std 1012–1986, with the exceptions stated in the Regulatory Position, 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 in Appendix B, as applied to software verification and validation. 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. IEEE Std 1028–1988 provides an approach that is acceptable to the NRC staff for carrying out software reviews, inspections, walkthroughs, and audits subject to certain provisions.

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 experience, and they 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 verification and validation (V&V), reviews, and audits are important parts of the effort to achieve compliance with the NRC's requirements. Software engineering practices rely, in part, on software V&V and on technical reviews and audits 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 II, III, XI, and XVIII of Appendix B. In addition, management reviews and audits of software processes are part of a verification process consistent with Criterion I of Appendix B.

General design verification requirements, but not details of software V&V planning and the conduct of reviews and audits, are described by IEEE Std 7–4.3.2–1993, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,"[3] which is endorsed by Revision 1 of Regulatory

[4]The 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."

Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," and ASME/NQA–1–1994, "Quality Assurance Requirements for Nuclear Facility Applications." Two consensus standards on software engineering, IEEE Std 1012–1986 (reaffirmed in 1992) and IEEE Std 1028–1988 (reaffirmed in 1993), describe the software industry's approaches to software verification, validation, review, and audit activities that are generally accepted in the software engineering community. Compliance with these standards helps to meet regulatory requirements by ensuring that disciplined software V&V, review, and audit practices accepted within the software community will be incorporated into software processes applied to safety system software. IEEE Std 1012–1986 describes the elements of a software V&V plan and, for software deemed "critical software" by IEEE Std 1012–1986, describes a minimum set of V&V activities to be included in the plan. IEEE Std 1028–1988 is a process standard that provides guidance on how to conduct audits, inspections and walkthroughs, and technical and management reviews.

Technical reviews, some audits, and software inspections and walkthroughs are focused on the verification and validation of products of the software development process. Management reviews and other audits are focused on ensuring that planned activities are being accomplished effectively. Reviews and audits are closely associated with V&V activities since technical reviews and audits are frequently conducted by the V&V organization and because the V&V organization normally participates in management reviews. Because of this close connection of the V&V activity with reviews and audits, IEEE Std 1028–1988 and IEEE Std 1012–1986 are addressed together in this regulatory guide.

IEEE Std 603–1991 and IEEE Std 7–4.3.2–1993, which are endorsed by Revision 1 of Regulatory Guide 1.153 and Revision 1 of Regulatory Guide 1.152, respectively, do not provide for classification, although the foreword to IEEE Std 7–4.3.2–1993 recommends the addition of grading to future versions of IEEE Std 603. This regulatory guide is based on current standards and describes methods acceptable for any safety system software. Within the framework of the acceptable methods described by this regulatory guide, certain V&V activities are required. For smaller, less complex systems or components, these activities should require less effort. Additionally, the applicant or licensee determines how the required activities will be implemented, commensurate with the item's importance to safety. The benefits of this approach are that the concepts addressed in the standard are applied within the context of safety system development while the applicant or licensee has flexibility in implementation.

C. REGULATORY POSITION

The requirements specified in IEEE Std 1012–1986 provide an approach that is acceptable to the NRC staff for meeting the requirements of 10 CFR Part 50 and the guidance given in Revision 1 of Regulatory Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," as they apply to the verification and validation of safety system software, subject to the exceptions listed below in Regulatory Positions 1 through 8 and 11.

IEEE Std 1028–1988 provides an approach acceptable to the NRC staff for carrying out software reviews, inspections, walkthroughs, and audits, subject to the exceptions listed below in Regulatory Positions 9 through 11. These are often performed in association with V&V or software quality assurance activities. Except as noted below, the appendices to these standards 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 of 10 CFR Part 50 as ensured by complying with the criteria of Appendix B applied to the verification, validation, reviews, and audits 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. CRITICAL SOFTWARE

IEEE Std 1012–1986 refers to critical and noncritical software. It defines the contents of a Software V&V Plan (SVVP) for all software and, for critical software, identifies a minimum set of software V&V tasks and their inputs and outputs that must be included in the SVVP. Critical software is defined in IEEE Std 1012–1986 to be software whose failure could have an impact on safety or could cause large financial or social loss. For the purposes of this regulatory guide, critical software means software used in nuclear power plant safety systems per footnote 4 of this guide, a narrower set of critical software than that defined in IEEE Std 1012–1986.

2. SOFTWARE RELIABILITY

In its discussion of component and integration test plans in Table 1, IEEE Std 1012–1986 identifies measurement of software reliability as a criterion for

determining whether software elements correctly implement software requirements. The following is noted in Revision 1 of Regulatory Guide 1.152.

> Section 5.15, "Reliability," of IEEE Std 7–4.3.2–1993 states, "When qualitative or quantitative reliability goals are required, the proof of meeting the goals shall include software used with the hardware." The staff does not endorse the concept of quantitative reliability goals as a sole means of meeting the Commission's regulations for reliability of the digital computers used in safety systems.

3. INDEPENDENCE OF SOFTWARE V&V

IEEE Std 1012–1986 does not require independence in the performance of software V&V, but the NRC does require independence. Criterion III, "Design Control," imposes an independence requirement for the verification and checking of the adequacy of the design, requiring that those who perform the verification and checking be different from those who accomplish the design. Approaches to performing independent software V&V are described in Revision 1 of Regulatory Guide 1.152. Regardless of the approach selected for a given V&V task, the responsibility for the adequacy of V&V lies with the organization responsible for the independent V&V. The person accountable for V&V must also be independent of the person accountable for the design. This independence must be sufficient to ensure that the V&V process is not compromised by schedule and resource demands placed on the design process. The independent verifiers must be sufficiently competent in software engineering to ensure that software V&V is adequately implemented. Criterion II, "Quality Assurance Program," states that the program must provide for indoctrination and training of personnel performing activities affecting quality as necessary to ensure that suitable proficiency is achieved and maintained. It is beneficial if the independent verifiers are also knowledgeable regarding nuclear applications.

4. DESIGN CHANGES

IEEE Std 1012–1986, in paragraph 3.7.2, requires a description in the SVVP of the criteria for determining the extent to which a V&V task must be reperformed following a change to an input of the task. The criteria described in the SVVP must be consistent with Criterion III, "Design Control," which requires that design changes be subject to design control measures commensurate with those applied to the original design. In addition, IEEE Std 1012–1986 includes cost and schedule as possible criteria for determining the extent of re-performance of V&V tasks. Such cost and schedule criteria, if used, must be commensurate in importance with the cost and schedule criteria that applied to verification of the original design. Any use of these criteria must be consistent with the requirement of 10 CFR 50.57(a)(3) that there be reasonable assurance that the activities authorized by the operating license can be conducted without endangering the health and safety of the public.

5. CONFORMANCE OF MATERIALS

Criterion III, "Design Control," states that measures are to be established for the selection and review for suitability of application of materials, parts, equipment, and processes that are essential to the safety-related functions of the structures, systems, and components. Criterion VII, "Control of Purchased Material, Equipment, and Services," states that measures are to be established to ensure that purchased material, whether purchased directly or through contractors and subcontractors, conform to the procurement documents. In its discussion of V&V during the operation and maintenance phase of the software life cycle, IEEE Std 1012–1986 (in paragraph 3.5.8) provides requirements and guidance for retrospective V&V of software that was not verified under the standard. The use of this guidance for the acceptance of pre-existing (e.g., commercial off-the-shelf) critical software not verified during development to the provisions of this regulatory guide or its equivalent is not endorsed. Revision 1 of Regulatory Guide 1.152 provides information on the acceptance of pre-existing software. Additional detailed information on acceptance processes is available in EPRI TR–106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications" (October 1996). [5]

6. QUALITY ASSURANCE

Criterion I identifies the quality assurance functions of (a) assuring that an appropriate quality assurance program is established and effectively executed and (b) verifying, such as by checking, auditing, and inspecting, that activities affecting the safety-related functions have been correctly performed. Criterion XVII requires that sufficient records be maintained to furnish evidence of activities affecting quality. Criterion III requires that design changes be subject to design

[5]Electric Power Research Institute documents may be obtained from the EPRI Distribution Center, 207 Coggins Drive, P.O. Box 23205, Pleasant Hill, CA 94523. EPRI TR–106439 is also available for inspection or copying for a fee in 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.

control measures commensurate with those applied to the original design. In addition to the requirements of IEEE Std 1012–1986 (in paragraph 3.7.4) regarding control procedures, any V&V materials necessary for the verification of the effectiveness of the V&V programs or necessary to furnish evidence of activities affecting quality must be maintained as quality assurance records. Those materials necessary for the reverification of changes must be maintained under configuration management.[6]

7. TOOLS FOR SOFTWARE DEVELOPMENT

Tools used in the development of safety system software should be handled according to IEEE Std 7–4.3.2–1993, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," as endorsed by Revision 1 of Regulatory Guide 1.152. IEEE Std 7–4.3.2–1993 states that "V&V tasks of witnessing, reviewing, and testing are not required for software tools, provided the software that is produced using the tools is subject to V& V activities that will detect flaws introduced by the tools." If this cannot be demonstrated, the provisions of this Regulatory Guide 1.168 are applicable.

8. V&V TASKS

Table 2 of IEEE Std 1012–1986 lists optional V&V tasks. These are further described in the appendix (which is for information only) to IEEE Std 1012–1986. These tasks are intended to provide a tailoring capability by allowing tasks to be added to the minimum set for critical software. Exception is taken to the 'optional' status of some tasks on this list; they are considered by the NRC staff to be acceptable methods for meeting the requirements of Appendices A and B to 10 CFR Part 50 as applied to software, regardless of whether they are performed by the V&V organization. The following tasks are considered by the NRC staff to be part of the minimum set of V&V activities for critical software unless they are (1) incorporated into other V&V tasks in the SVVP or (2) performed outside the software V&V organization as part or all of the duties of some other organization.

8.1 Configuration Management

Configuration management (CM), and software configuration management in particular, are not optional functions, but are identification and control functions considered to be mandatory under Criterion VIII, "Identification and Control of Materials, Parts, and Components," as applied to software. The same personnel who perform the V&V functions may perform the software configuration management functions.

8.2 Audits

Criteria III, "Design Control," and XVIII, "Audits," require the performance of audits. These audits include functional audits, in-process audits, and physical audits for software. These audits are commonly considered to be the responsibility of the software quality assurance organization and the configuration management organization, but they may be handled by the V&V organization. If so, the audits should be described in the SVVP. An acceptable method of conducting these audits is described in IEEE Std 1028–1988.

8.3 Regression Analysis and Testing

Criterion III, "Design Control," requires that design changes be subject to design control measures commensurate with those applied to the original design. Regression analysis and testing following the implementation of software modifications is a necessary element of the V&V of software changes. It is considered by the staff to be part of the minimum set of software V&V activities for critical software.

8.4 Installation and Checkout Testing

Criterion XI, "Test Control," requires that the test program include, as appropriate, proof tests prior to installation, pre-operational tests, and operational tests. The user of IEEE Std 1012–1986 must identify in the SVVP which tests will be performed to meet Criterion XI.

8.5 Test Evaluation

Test evaluation, an optional task described in the Appendix to IEEE Std 1012–1986, calls for confirmation of the technical adequacy of test materials such as plans, designs, and results. The evaluation of these materials is necessary for consistency with Criterion II, "Quality Assurance Program," in its requirement for controlled conditions and with Criterion XI, "Test Control," in its requirement for the evaluation of test results.

8.6 Evaluation of User Documentation

Table 2 of IEEE Std 1012–1986 includes User Documentation Evaluation as an optional V&V task. The requirements of Criterion III, "Design Control," for verifying and checking the design apply to software documentation, including user documentation.

[6]See the guidance in Regulatory Guide 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

9. CLARIFICATIONS

Criterion III, "Design Control," requires measures, such as the performance of design reviews, to be provided for verifying or checking the adequacy of the design, and Criterion II, "Quality Assurance Program," requires activities affecting quality to be accomplished under suitably controlled conditions. Criterion V, "Instructions, Procedures, and Drawings," requires activities affecting quality to be directed by written instructions, procedures, and drawings that include acceptance criteria for determining that these activities are successfully accomplished. IEEE Std 1028–1988 contains a mix of verbs (such as "will," variants of "to be," or verbs used in the present tense (as described below)), and it may not be clear whether the usage is intended to be a requirement of the standard or a statement of fact. In this regulatory guide, the following are considered to be conditions for audits and reviews.

9.1 The responsibilities and prerequisites of sections 3.1 and 3.2 and the minimum process description template of section 3.3 of IEEE Std 1028–1988.

9.2 Anything with the terms "must," "required," "shall," "minimum requirements," "is responsible for," "will ensure," "is to (or 'is not allowed to')," "minimum input," "necessary input," "is conducted when," "reports that identify (or 'contain')," "output is," or variations of any of these terms.

9.3 The responsibilities, minimum inputs, entry and exit criteria, procedures, and auditability of items described in sections 4 through 8 of IEEE Std 1028, unless the IEEE Std 1028–1988 phraseology indicates a recommended or optional item.

10 TABLE 1 IN IEEE STD 1028–1988

In Table 1 in IEEE Std 1028–1988, the word 'include' in the column heading means representative but not exhaustive. Table 1 relates quality assurance processes to quality assurance objectives, adds 'test' for completeness, and matches key processes to quality assurance objectives. In so doing, it does not provide an exhaustive list of all process and objective relationships. In particular, the relationship of testing to verification is not indicated, but this relationship is added by this regulatory guide.

11. OTHER CODES AND STANDARDS

Various sections of IEEE Std 1012–1986 and IEEE Std 1028–1988 reference other industry codes and 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 the issuance of this guide.

Except in those cases in which an applicant or licensee 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 who propose system modifications that are voluntarily initiated by the licensee if there is a clear nexus between the proposed modifications and this guidance.

BIBLIOGRAPHY

Hecht, H., A.T. Tai, K.S. Tso, "Class 1E Digital Systems Studies," NUREG/CR–6113, USNRC, October 1993.[1]

Hecht, H., et al., "Verification and Validation Guidelines for High Integrity Systems," NUREG/CR–6293, USNRC, March 1995.[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.[1]

[1]Copies 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.

[2]Single 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–1054, "Verification, Validation, Reviews, and Audits 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

☆ U.S. GOVERNMENT PRINTING OFFICE: 1997 417-801/60035