U.S. NUCLEAR REGULATORY COMMISSION
OFFICE OF NUCLEAR REGULATORY RESEARCH

January 2003
Division 1

DRAFT REGULATORY GUIDE

Contact: R. Shaffer (301)415-7606

DRAFT REGULATORY GUIDE DG-1123

VERIFICATION, VALIDATION, REVIEWS, AND AUDITS FOR DIGITAL COMPUTER SOFTWARE USED IN SAFETY SYSTEMS OF NUCLEAR POWER PLANTS

(Proposed Revision 1 of Regulatory Guide 1.168)

A. INTRODUCTION

In 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," paragraph 50.55a(a)(1) requires, in part, that structures, systems and components be designed, tested, and inspected to quality standards commensurate with the importance of 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, 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 structures, systems and components that prevent or mitigate the consequences of postulated accidents. In particular, besides the structures, 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 structures, systems and components, such as designing, purchasing, installing, testing, operating, maintaining, or modifying.

A specific requirement is contained in 10 CFR 50.55a(h) that protection systems in nuclear power plants with construction permits issued after January 1, 1971, but before May 13, 1999, must meet the requirements stated in either IEEE Std 279, "Criteria for

Protection Systems for Nuclear Power Generating Stations,"[1] or in IEEE Std 603-1991, "Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995.[2] Protection systems in nuclear power plants with construction permits issued before January 1, 1971, must be consistent with their licensing basis or may meet the requirements of IEEE Std 603-1991 and the correction sheet dated January 30, 1995. Protection systems in applications filed on or after May 13, 1999, must meet the requirements for safety systems in IEEE Std 603-1991 and the correction sheet dated January 30, 1995. Clause 4.3 of IEEE Std 279-1971 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. Clause 5.3 of IEEE Std 603-1991 states that components and modules (of safety systems) must be of a quality that is consistent with minimum maintenance requirements and low failure rates. Safety system equipment must be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program. (See ASME Std NQA-1-1989.) Note that guidance on the application of these criteria for safety system equipment employing digital computers and programs or firmware is found in IEEE Std 7-4.3.2-1993, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," which is endorsed by Regulatory Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants."

In Appendix B, 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) ensure that an appropriate quality assurance program is established and effectively executed and (b) 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 1012-1998, "IEEE Standard for Software Verification and Validation," and IEEE Std 1028-1997, "IEEE Standard for Software

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

[2] Revision 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.

Reviews and Audits." IEEE Std 1012-1998, 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.[3] 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. If those systems include software, the requirements extend to the software elements. IEEE Std 1028-1997 provides guidance 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, Section 7.0, "Instrumentation and Controls," NUREG-0800, Revised June 1997. 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 conform with the revised Chapter 7 of the Standard Review Plan.

Regulatory guides are issued to describe to the public methods acceptable to the NRC staff for implementing specific parts of the NRC's regulations, to explain techniques used by the staff in evaluating specific problems or postulated accidents, and to provide guidance to applicants. Regulatory guides are not substitutes for regulations, and compliance with regulatory guides is not required. Regulatory guides are issued in draft form for public comment to involve the public in developing the regulatory positions. Draft regulatory guides have not received complete staff review; they therefore do not represent official NRC staff positions.

The information collections contained in this draft regulatory guide are covered by the requirements of 10 CFR Part 50, which were approved by the Office of Management and Budget (OMB), approval number 3150-3011. The NRC may not conduct or sponsor, and a person is not required to respond to, a request for information or an information collection requirement unless the requesting document displays a currently valid OMB control number.

B. DISCUSSION

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

[3] The term "safety systems" is synonymous with "safety-related systems." The General Design Criteria cover structures, systems 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."

safety system software, software verification and validation (V&V), reviews, and audits are important parts of the effort to achieve compliance with NRC 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, which is endorsed by Revision 1 of Regulatory Guide 1.152, and ASME/NQA-1-1994, "Quality Assurance Requirements for Nuclear Facility Applications." Two consensus standards on software engineering, IEEE Std 1012-1998 and IEEE Std 1028-1997 (reaffirmed in 2002), describe the software industry's approaches to software verification, validation, review, and audit activities that are generally accepted in the software engineering community. Meeting 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 1012-1998 describes the process of software V&V, including elements of a software V&V plan, and describes a minimum set of V&V activities for software at different integrity levels. IEEE Std 1028-1997 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 1028-1997 and IEEE Std 1012-1998 are addressed together in this regulatory guide.

Additional guidance on conducting software reviews can be found in the annexes to IEEE Std 1028-1997. Annex A lists different review titles, and shows which of the five review types in the standard are appropriate to use with each review title. For example, a Software Requirements Review may be carried out using the IEEE Std 1028-1997 Technical Review. Annex B to IEEE Std 1028-1997 compares the five review types according to various characteristics of the review types, and provides guidance in choosing a review type.

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. IEEE 1012-1998 provides a method of grading termed "integrity levels." The activities in IEEE Std 1012-1998, and the effort to be expended on these activities, depends on the integrity level of the software. Safety system software entails the largest number of activities and the most effort for each activity. Systems with lower consequences in the case of failure should require fewer activities and less effort.

This regulatory guide is based on current standards and describes methods acceptable for any safety system software. This regulatory guide discusses certain required V&V activities. 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 1012-1998, "IEEE Standard for Software Verification and Validation," provide methods that are 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 in Regulatory Positions 1 through 8.

The methods in IEEE Std 1028-1997, "IEEE Standard for Software Reviews and Audits," provide an approach acceptable to the NRC staff for carrying out software reviews, inspections, walkthroughs, and audits, subject to the exceptions listed below in Regulatory Position 8. These are often performed in association with 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.

1. CRITICAL SOFTWARE

IEEE Std 1012-1998 defines a four-level method of quantifying software criticality, in which level 4 is the highest and level 1 the lowest (Clause 4.1). IEEE Std 1012-1998 requires the applicant or licensee either to use the method in the standard or to define another method and provide a mapping between the applicant or licensee's method and the method defined in the standard. Software used in nuclear power plant safety systems should be assigned integrity level 4. Some systems important to safety may be assigned lower levels if the assignment can be justified. The staff recommends that integrity levels be assigned for software in systems important to safety as well as for safety system software.

2. SOFTWARE RELIABILITY

In its discussion of component and integration test plans in Table 1 (Activity 5.4.3, "Design V&V Activity," tasks (5), "Component V&V Test Plan Generation and Verification," and (6), "Integration V&V Test Plan Generation and Verification"), IEEE Std 1012-1998 identifies measurement of software reliability as a criterion for determining whether software elements correctly implement software requirements.

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 NRC's regulations for reliability of the digital computers used in safety systems.

This statement is also in Revision 1 of Regulatory Guide 1.152.

3. INDEPENDENCE OF SOFTWARE VERIFICATION AND VALIDATION

Criterion I, “Organization,” requires that persons and organizations performing quality assurance functions report to a management level such that sufficient authority and organization freedom exist, including sufficient independence from cost and schedule limitations. Quality assurance functions include “verifying, such as by checking, auditing and inspection, that activities affecting the safety-related functions have been correctly performed.” 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 persons other than those who accomplish the design. A method of performing independent software V&V is described in Revision 1 of Regulatory Guide 1.152. A different method is described in IEEE Std 1012-1998 in Clause 7.4.1 and Annex C.

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 is to 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.

IEEE Std 1012-1998 provides guidance on determining financial, managerial, and technical independence requirements for software V&V. Financial and managerial independence are required by Appendix B, Criterion I. Technical independence is required by Appendix B, Criterion III. The staff recommends that these three types of independence be achieved.

Note that Clause C.4.1 of IEEE Std 1012-1998, Annex C, states that the V&V responsibility “is vested in an organization that is separate from the development organization.” The NRC staff position is that this does *not* require that a separate company perform independent V&V; a separate organization within a company will satisfy this clause provided that adequate independence requirements are met.

4. 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, conforms to the procurement documents. In its discussion of V&V during the operation and maintenance phase of the software life cycle, IEEE Std 1012-1998 (in Clauses 1.2, 1.4, and 4.1 and

Table 1 Activity 5.6.1 Task 1, all of which reference Annex D, “V&V of Reusable Software”) provides guidance for retrospective V&V of software that was not verified under the standard. The NRC staff does not endorse the use of this guidance for the acceptance of pre-existing (e.g., commercial off-the-shelf) critical software not verified during development. 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. QUALITY ASSURANCE

Criterion I identifies the quality assurance functions of (a) ensuring 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 control measures commensurate with those applied to the original design. In addition to the requirements of IEEE Std 1012-1998 (in Clause 7.7.4) 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 should be maintained as quality assurance records. The materials necessary for the reverification of changes must be maintained under configuration management.

6. 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, 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.

7. VERIFICATION AND VALIDATION TASKS

Table 3 of IEEE Std 1012-1998 lists optional V&V tasks. These are further described in Annex G (which is for information only) to IEEE Std 1012-1998. 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.

7.1 Audits

Criterion III, “Design Control,” and Criterion XVIII, “Audits,” require the performance of audits. These audits include functional audits, in-process audits, and physical audits of 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 1028-1997.

7.2 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 an 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 safety system software.

7.3 Security Assessment

A security breach of a digital system containing safety system software has the potential to prevent that software from fulfilling its safety function. In Appendix A, Criteria 21, 25, and 29 require that certain safety systems have an extremely high probability of accomplishing their safety functions. According to 10 CFR 73.46, components must be protected by physical barriers and access control. The NRC staff considers security assessment of safety system software to be part of the minimum set of software V&V activities for such software.

7.4 Test Evaluation

Test evaluation, an optional task described in the Appendix to IEEE Std 1012-1998, calls for confirmation of the technical adequacy of test materials such as plans, designs, and results. These materials are evaluated 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.

7.5 Evaluation of User Documentation

Table 2 of IEEE Std 1012-1998 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.

8. OTHER CODES AND STANDARDS

Various sections of IEEE Std 1012-1998 and IEEE Std 1028-1997 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 draft regulatory guide. No backfitting is intended or approved in connection with the issuance of this guide.

This draft guide has been released to encourage public participation in its development. 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 to be described in the active guide reflecting public comments 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

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

2. Hecht, H., et al., "Verification and Validation Guidelines for High Integrity Systems," NUREG/CR-6293, Volumes 1 and 2, USNRC, March 1995.

3. 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.

4. Lawrence, J.D., and G.G. Preckshot, "Design Factors for Safety-Critical Software," NUREG/CR-6294, USNRC, December 1994

5. Seth, S., et al., "High Integrity Software for Nuclear Power Plants: Candidate Guidelines, Technical Basis and Research Needs," NUREG/CR-6263, Volumes 1 and 2, USNRC, June 1995.

E. REGULATORY ANALYSIS

PROBLEM

Because traditional and well-understood methods of design and quality assurance for developing and manufacturing hardware apply imperfectly to software design and development, additional guidance beyond standard approaches for hardware is necessary if the intent of the NRC's regulations is to be achieved. This problem is faced in many industries where computers and software are replacing traditional hardware-only instrumentation and control (I&C) designs. To this extent, the nuclear industry is not very different from any industry associated with high-consequence hazards. While additional guidance is necessary to help prevent failures of digital I&C safety systems, the potential benefits of these systems make their use highly desirable.

The use of computers and software in safety-related I&C designs is part of the larger problem of ensuring long-term safety of nuclear power plants, and it is seen as part of the solution as well. It is not just digital systems themselves that give rise to concerns about design verification and quality assurance, but the increase in complexity of the system designs (including software) being attempted is also a factor. The NRC staff discussed its concerns in SECY 91-292, "Digital Computer Systems for Advanced Light Water Reactors," and again in parts of SECY 93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." Subsequently, the NRC staff sponsored studies that resulted in characterization of design factors, guidelines, technical bases, and practices generally considered appropriate for high-integrity software [see NUREG/CR-6101, "Software Reliability and Safety in Nuclear Reactor Protection Systems (November 1993); NUREG/CR-6113, "Class 1E Digital Systems Studies" (October 1993); NUREG/CR-6263, "High Integrity Software for Nuclear Power Plants: Candidate Guidelines, Technical Basis and Research Needs (June 1995); NUREG/CR-6293, "Verification and Validation Guidelines for High Integrity Systems" (March 1995); and NUREG/CR-6294, "Design Factors for Safety-Critical Software" (December 1994)]. These studies identified software design control techniques that are currently being used in "best practice" software development efforts. While it is possible to simply list the criteria covered, the problem still remains of reaching a common understanding between the NRC staff and industry practitioners regarding what constitutes acceptable software engineering practice for safety systems. An agreed-upon collection of standards, established practice, and engineering techniques for software engineering methods is needed to complement the collection that already supports traditional hardware engineering methods, such as statistical quality control, testing standards, and quality assurance techniques used on design and manufacturing processes for hardware components.

Software verification and validation (V&V) is fundamental to the assurance of software quality, as evidenced by the large body of literature on the subject. An effective V&V program depends on careful planning and execution and this, in turn, depends partially on appropriate documentation. For systems and components under its purview, Appendix B to 10 CFR Part 50 requires design control, including the use of written design control procedures, including design reviews and testing, and documentation of results, as well as the maintenance of sufficient records to furnish evidence of activities affecting quality. The importance of software V&V in the development of high-integrity software is stressed in the studies cited above. NUREG/CR-6101, in its description of activities and related documents necessary for the production of reliable software, addresses software V&V in all software life cycle phases. A common understanding between the staff and

applicants of an acceptable method for accomplishing software V&V will benefit staff safety reviews significantly, and the technical basis for such an understanding exists. Therefore, software V&V documentation is an appropriate subject for staff review.

ALTERNATIVE APPROACHES

Based on the studies referenced above, consensus in the software engineering community is sufficient to ensure widespread familiarity and reasonable levels of agreement. Two approaches were considered, taking no action and adopting recent revisions to the two IEEE standards.

The first alternative, taking no action, will continue NRC endorsement of two standards, IEEE Std 1012-1986 and IEEE Std 1028-1988. These standards have been replaced by IEEE with revised versions. Taking no action will thus fail to take advantage of the improvements in the revised versions of these standards.

VALUES AND IMPACTS

Values and impacts for each of the two identified approaches are analyzed below. In this analysis, the probability of the alternative approach having a positive effect on software quality and the probability of the effect of software quality on the achievement of overall safety goals are not known quantitatively. Although the current state of the art does not support quantitative estimates, the results of poor software quality are evident in notable instances of software failure in various industries. Therefore, a positive correlation between software quality and the achievement of safety goals is inferred from the instances of negative effects of poor software quality, i.e., software quality is a necessary but insufficient factor in achieving safety goals. In the summary below, an impact is a cost in schedule, budget, or staffing or an undesired property or attribute that would accrue from taking the proposed approach. Both values and impacts may be functions of time.

Alternative 1, Take No Action

Presently license reviews of safety software V&V entail confirming that the plan for V&V activities conforms with Reg Guide 1.168 and then confirming that the licensee or applicant implemented that plan appropriately. Because the 1987 version of IEEE Std 1012 and 1988 version of the IEEE Std 1028 that are endorsed by RG 1.168 provide only guidance for planning V&V process and the SRP provides general guidance on implementing that planned V&V process, the NRC staff and licensees / applicants might interpret differently the types and amount of V&V activities necessary to implement the V&V plan properly.

Alternative 2, Endorse Revised Software Engineering Standards

The 1997 version of IEEE Std 1012 and the 1998 version of IEEE Std 1028 provides guidance in addition to the V&V plan, including guidance on the types and amount of V&V activities necessary to implement the V&V plan properly. Therefore, updating RG 1.168 be endorsing the new version of the IEEE standards will (1) simplify the staff's review process and enable licensees/applicants to develop a unified coherent means of meeting the requirements of 10 CFR Part 50 and (2) reduce regulatory

uncertainty and thereby help to minimize the costs associated with the implementation of this guide. As a result, the costs associated with the implementation of this guide are expected to be minimal.

CONCLUSIONS

There are a number of potential benefits associated with the use of digital I&C safety systems in nuclear power plants. Implementations of these systems must be consistent with the Commission's regulations. Two approaches to providing additional guidance for software were examined. Endorsing the revised software engineering standards has good value with minimal impact and addresses the stated problem. Note that these endorsements present no new regulatory requirements; they define acceptable approaches for meeting existing requirements.

DECISION/RATIONALE

Based on the lowest impact and highest value for problem solution capability, the second alternative, endorsing the revised software engineering standards, has been chosen. The highest value will be achieved by selecting standards that address software engineering processes that have a high potential for ensuring that safety system software meets the requirements of the NRC's regulations as they are applied to software. Standards should be selected based on relevance and maturity.