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

DRAFT REGULATORY GUIDE

August 1996
Division 1
Draft DG-1054

Contact: J. Kramer (301)415-5891

DRAFT REGULATORY GUIDE 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,

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

DF02
0/1

This regulatory guide is being issued in draft form to involve the public in the early stages of the development of a regulatory position in this area. It has not received complete staff review and does not represent an official NRC staff position.

Public comments are being solicited on the draft guide (including any implementation schedule) and its associated regulatory analysis or value/impact statement. Comments should be accompanied by appropriate supporting data. Written comments may be submitted to the Rules Review and Directives Branch, DFIPS, Office of Administration, U.S. Nuclear Regulatory Commission, Washington, DC 20555. Copies of comments received may be examined at the NRC Public Document Room, 2120 L Street NW., Washington, DC. Comments will be most helpful if received by **October 31, 1996.**

Requests for single copies of draft guides (which may be reproduced) or for placement on an automatic distribution list for single copies of future guides in specific divisions should be made in writing to the U.S. Nuclear Regulatory Commission, Washington, DC 20555, Attention: Office of Administration, Distribution and Mail Services Section.

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.

Many of the criteria in Appendix B,[1] "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," to 10 CFR Part 50 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) 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 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 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 be provided 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.

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

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

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 provisions 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 of 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 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, currently under revision), which is used by the Office of Nuclear Reactor Regulation in the review of applications to construct and operate nuclear power plants. This draft regulatory guide will apply to Chapter 7 of that document.

Regulatory guides are issued to describe and make available to the public such information as methods acceptable to the NRC staff for implementing specific parts of the NRC's regulations, techniques used by the staff in evaluating specific problems or postulated accidents, and 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 the early stages of developing the regulatory positions. Draft regulatory guides have not received complete staff review and 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, 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.

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

B. DISCUSSION

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

Software incorporated into instrumentation and control systems covered by Appendix B will be referred to in this regulatory guide as safety system software. For safety system software, software 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 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.

C. REGULATORY POSITION

The requirements[5] specified in IEEE Std 1012-1986 provide an approach 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 provisions 1 through 8 and 11, listed below.

IEEE Std 1028-1988 provides an approach acceptable to the NRC staff for carrying out software reviews, inspections, walkthroughs, and audits, subject to provisions 9 through 11, listed below. 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 provisions are necessary and will be considered by the NRC staff in the review of applicants' submittals as described by the Standard Review Plan, which is currently under revision.

---

[5] In this regulatory guide, the term "requirements" refers to requirements imposed by the NRC's regulations as well as to requirements that must be met in order to comply with a standard.

1. 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 it means safety system software as per footnote 4.

2. 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. The NRC staff's acceptance of the reliability of the computer system is based on deterministic criteria for both the hardware and software rather than on quantitative reliability goals.
>
> Software failures that are not the consequence of hardware failures are caused by design errors and, therefore, do not follow the random failure behavior used for hardware reliability. The NRC staff believes that quantitative reliability determination, using a combination of analysis, testing, and operating experience, provides information regarding the safety importance of the computer system and also provides an added level of confidence in its reliable performance. If quantitative software reliability goals are used, the staff believes that the amount of testing of the safety system instrumentation and control equipment will increase. The staff recognizes that the commercial dedication of "commercially" available digital systems in nuclear applications relies a great deal on quantitative methods because of the operating experience data (such as number of hours of successful operation) accumulated over the years. The staff does not intend to preclude operating experience data from the justification of a successful commercial dedication.

3. IEEE Std 1012-1986 does not require independence in the performance of software V&V. 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. Therefore, independence is an additional requirement for software V&V, applying to personnel performing software V&V and software design, so that those who perform software V&V must be different from those who design or code the software. 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 also be as proficient in software engineering as the software developer; 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. 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 re-performed 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. 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.

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 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.*

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 are applicable.

---

*idance is being developed on this subject in Draft Regulatory Guide DG-1055, "Configuration Management ans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

8. 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 necessary 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.

9. 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.

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. 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. 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 proposed guide. Any backfitting that may result from applying this new guidance to operating plants would be justified in accordance with established NRC backfitting guidance and procedures.

This draft guide has been released to encourage public participation in its development. Except in those cases in which an applicant proposes an acceptable alternative method for complying with specified portions of the NRC's regulations, the method 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, standard design certifications and design approvals, and combined operating licenses. The active guide will also be used to evaluate submittals from operating reactor licensees who propose modifications that go beyond the current licensing basis if those modifications are voluntarily initiated by the licensee and there is a clear connection between the proposed modifications and this guidance. This guide will be used in conjunction with, and will eventually be reflected in, the Standard Review Plan, which is currently under revision.

REGULATORY ANALYSIS

1. 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 the 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,"[1] and again in parts of SECY 93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs."[1] 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"

[1]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; telephone (202)634-3273; fax (202)634-3343.

(December 1994)].[2] These studies identified software design control techniques that are currently being used in "best practice" software development efforts. While it is possible simply to 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) and the related review and audit techniques are fundamental to the assurance of software quality, as evidenced by the large body of literature on the subjects. Appendix B to 10 CFR Part 50 requires design control, including design verification, for structures, systems, and components under its purview. The importance of software V&V to high integrity software is stressed in the studies referenced above. NUREG/CR-6101 includes V&V, review, and audit activities throughout the software life cycle in its description of activities and related documents necessary for the production of reliable software. According to NUREG/CR-6263, "The relationship of software V&V to safety is that V&V reduces the likelihood of errors. Individual V&V activities form a chain of arguments whose conclusion is that the system performs according to specifications. However, V&V cannot guarantee safety. Confidence in the safety of a software system depends to a considerable extent on how thoroughly the V&V activities have demonstrated that the source code, software design, and software requirements have satisfied those system safety requirements allocated to the software." It also states, "A V&V plan is the starting point in the chain of V&V activities that span the life cycle. Therefore, it can compromise the entire V&V effort, and thus the safety system software, if it is inadequate."

---

[2]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 also 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; telephone (202)634-3273; fax (202)634-3343.

2. ALTERNATIVE APPROACHES

Based on the studies referenced above, an alternative was identified in which consensus in the software engineering community is sufficient to ensure widespread familiarity and reasonable levels of agreement. There are two additional approaches, taking no action and prescribing a detailed approach built from staff selections of best practice. In all, three approaches were identified:

1. Take no action,
2. Prescribe a detailed approach,
3. Endorse one or more software engineering standards.

The first alternative, taking no action, has the attraction that its initial cost is low since there are no "start-up" activities. It has flexibility, since each applicant would develop its own technical basis demonstrating that its digital system, and the quality assurance measures applied to it, complied with the NRC's regulations. However, this could have adverse effects on the level of staff effort required to conduct reviews or to ensure consistency among reviews. In the absence of an identified set of commonly accepted guidelines, practices, and quality assurance measures applicable to software engineering, NRC staff review would take longer and require greater effort to ensure consistent staff safety evaluations. From the applicant's perspective, this flexibility also has associated potential costs because there could be more unknowns associated with demonstrating compliance with regulations. Although the initial cost would apparently be low, taking no action could result in greater total costs, to both the NRC staff and the applicant, during the safety evaluation process.

Prescribing a detailed approach could have significant preliminary costs involved in formulating the approach and dealing with the public comment that would inevitably result. The staff has been reluctant in the past to take this approach. Such an approach places the staff in the position of designer and compromises, or appears to compromise, the staff's independence as design safety reviewers; this is not the role of the regulator.

Consensus standards on software development are available and represent current good practice as agreed upon by responsible professionals in the software industry. Many organizations issuing standards, such as the IEEE and ANSI, provide for review and revision of standards at regular intervals to

ensure the consensus positions are current. In the United States, the Institute of Electrical and Electronic Engineers (IEEE), the American Nuclear Society (ANS), the Electronic Industry Association (EIA), the Instrument Society of America (ISA), the American Society of Mechanical Engineers (ASME), and the American National Standards Institute (ANSI) are the standards bodies issuing software engineering standards, computer standards, or related quality standards. In Europe, the International Electrotechnical Commission (IEC), the International Organization for Standardization (ISO), the International Atomic Energy Agency (IAEA), and the Comité Consultatif International Télégraphique et Téléphonique (CCITT) fill the same roles. The European Committee for Electrotechnical Standardization (CENELEC), a regional standardization body, adopts national and international standards. The overall collection of standards issued by these bodies covers a variety of subjects considered important to software quality. The standards specific to the nuclear industry issued by the U.S.-based organizations are, in general, compatible with the NRC's regulations. The software engineering standards issued by these organizations, notably the IEEE software engineering standards, are in general compatible with nuclear-industry-specific standards. Together, these standards form a framework for addressing the use of software within nuclear systems in the U.S. nuclear regulatory environment. Selected international standards can complement this framework; however, they tend to be organized differently and do not map directly into the U.S. industry-specific framework.

3. VALUES AND IMPACTS

Values and impacts for each of the three identified approaches are analyzed below. In this analysis, the probability of an 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.

3.1 Alternative 1 -- Take No Action

If no action is taken, retaining the status quo, the NRC staff will continue to receive applications or requests to review safety questions that are prepared with no clear guidance on what the staff considers to be acceptable methods of ensuring that safety-related software meets the requirements of the NRC's regulations. Each applicant would propose measures it deems necessary, and these measures will be reviewed by the staff and discussed with the applicant to reach a resolution that is acceptable to the staff and the applicant. This preserves the value of flexibility, but at the impact of additional staff and applicant effort and potential schedule extension. It is possible that a de facto staff position would develop from the accumulation of successful applications, but the amount of time and effort required to reach this condition is unknown.

Value - No value beyond the status quo

Impact - Schedule, budget, and staffing cost, to the staff and applicant, associated with regulatory uncertainty

3.2 Alternative 2 -- Prescribe a Detailed Approach

If the staff prescribed a detailed approach, applicants would enjoy regulatory certainty at the expense of reduced flexibility. Tangible immediate impacts would include staff time to specify and defend the approach in a public forum. Intangible impacts would include a potential compromise of staff effectiveness as impartial safety reviewers and a loss of input from innovative applicants. Future impacts would include maintenance of the approach as newer software engineering methods were developed by the technical community.

Values - Probable improvement in the likelihood of achieving safety goals as a consequence of staff expertise and specialized knowledge derived during the development of the prescribed approach

- Common understanding of regulatory view of software practice

Impacts
- Cost of staff effort to develop the approach
- Potential compromise of staff objectivity
- Innovative approaches discouraged as a result of increased cost
- Cost of evolving, maintaining, and communicating the approach

3.3 Alternative 3 - Endorse One or More Software Engineering Standards

If the staff endorses selected consensus software engineering standards, the staff and applicants obtain the benefit of the work of responsible software engineering professional standards committee volunteers. The value in this is the common understanding between the staff and applicants of an approach that has acceptance as good practice in the technical community. The standards usually permit tailoring to meet the needs of particular situations, so that a medium level of flexibility is retained. Additional staff effort is minimal, since members of the staff are already active in standards committees that the staff considers important to safety. Because detailed standards that address specific software engineering practices are available, the staff may select standards that address topics of particular importance regarding safety system software. Many standards, including IEEE software engineering standards, are reviewed and updated periodically, which acquaints the staff with changing practices. Coordination of standards efforts for standards used widely in the U.S. with international standards efforts is increasing, but the outcome of this is still unpredictable.

Values
- Probable improvement in the likelihood of achieving safety goals as a consequence of improvement in software practices
- Consideration of relevant topics
- Common understanding of good software practice, as defined by consensus processes in the software industry
- Maintenance and evolution of the definition of good software practice by the software industry

Impact
- Cost of endorsing the selected standards

4. 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. Three approaches to providing additional guidance for software were examined. Taking no action may result in accumulating regulatory expense as applicants submit proposed methods to assure the staff that safety-related software meets the requirements of the NRC's regulations. A de facto acceptable method would probably evolve, but the time and effort required for this to happen are unknown. A detailed staff prescription has unacceptable impacts and would involve the staff directly in the applicant's solution of technical problems. Endorsing selected software engineering standards has good value with minimal impact and addresses the stated problem. Note that none of these approaches presents new regulatory requirements; they define acceptable approaches for meeting existing requirements.

5. DECISION RATIONALE

Based on the lowest impact and highest value for problem solution capability, the third alternative, endorsing selected 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 applied to software. Standards should be selected based upon relevance and maturity.

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]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; 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, Attention: Distribution and Services Section, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001; or by fax at (301)415-2260. 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; telephone (202)634-3273; fax (202)634-3343.

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