



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

August 1996
Division 1
Draft DG-1059

DRAFT REGULATORY GUIDE

Contact: J. Kramer (301)415-5891

DRAFT REGULATORY GUIDE DG-1059

DEVELOPING SOFTWARE LIFE CYCLE PROCESSES FOR
DIGITAL COMPUTER SOFTWARE USED IN SAFETY SYSTEMS
OF NUCLEAR POWER PLANTS

A. INTRODUCTION

In 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," paragraph 55a(a)(1) requires, in part,¹ that systems and components be designed, tested, and inspected to quality standards commensurate with the safety function to be performed. Criterion 1, "Quality Standards and Records," of Appendix A, "General Design Criteria for Nuclear Power Plants," to 10 CFR Part 50 requires, in part,¹ that a quality assurance program be established and implemented in order to provide adequate assurance that systems and components important to safety will satisfactorily perform their safety functions. Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," to 10 CFR Part 50 describes criteria that a quality assurance program for systems and components that prevent or mitigate the consequences of postulated accidents must meet. In particular, besides the systems and components that directly prevent or mitigate the consequences of postulated accidents, the criteria of Appendix B also apply to all activities affecting the safety-related functions of such systems and components as designing, purchasing,

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

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 or active regulatory guides (which may be reproduced) should be made in writing to the U.S. Nuclear Regulatory Commission, Washington, DC 20555, Attention: Distribution and Mail Services Section, or by fax to (301)415-2260. Requests for placement on an automatic distribution list for single copies of future draft guides in specific divisions should be sent to the same address.

requirement is contained in 10 CFR 50.55a(h), which requires that reactor protection systems satisfy the criteria of IEEE Std 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations."² Paragraph 4.3 of IEEE Std 279-1971³ states that quality of components is to be achieved through the specification of requirements known to promote high quality, such as requirements for design, inspection, and testing.

Many of the criteria in Appendix B to 10 CFR Part 50 contain requirements closely related to software life cycle activities. Criterion I, "Organization," describes the establishment and execution of a quality assurance program. Criterion II, "Quality Assurance Program," states, in part, that activities affecting quality must be accomplished under suitably controlled conditions, which include assurance that all prerequisites for a given activity have been satisfied. This criterion also calls for taking into account the need for special controls and processes to attain the required quality. Criterion III, "Design Control," states, in part, that measures must be established for the identification and control of design interfaces and for coordination among participating design organizations. Criterion XV, "Nonconforming Materials, Parts, or Components," requires measures to be established to control materials, parts, or components that do not conform to requirements in order to prevent their inadvertent use or installation. Finally, Criteria VI, "Document Control," and XVII, "Quality Assurance Records," provide for the control of the issuance of documents, including changes thereto, that prescribe all activities affecting quality and provide for the maintenance of sufficient records to furnish evidence of activities affecting quality.

This regulatory guide endorses IEEE Std 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes,"³ subject to the provisions in the Regulatory Position. IEEE Std 1074-1995 describes a method acceptable to the NRC staff for complying with parts of the NRC's regulations for promoting high functional reliability and design quality in software used in safety systems.⁴ In particular, the method is consistent with the previously cited General Design Criteria and the criteria for quality assurance programs of Appendix B as they

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.

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."

apply to software development processes. 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.

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 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.

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. The development of software for high-integrity applications, such as safety system software, requires the use of a carefully planned and controlled

development process that incorporates the best available approaches to the various aspects of software engineering. There are a number of consensus standards that provide guidance on implementing currently accepted approaches to specific software engineering activities such as software requirements specification or software configuration management. A carefully planned and controlled software development effort must incorporate these specific activities into an orderly process to be followed in the software life cycle, including pre-software-development and post-software-development processes. This regulatory guide addresses the subject of designing software life cycle processes appropriate for the development of safety system software.

IEEE Std 1074-1995 describes, in terms of inputs, development, verification or control processes, and outputs, a set of processes and constituent activities that are commonly accepted as composing a controlled and well-coordinated software-development process. It describes inter-relationships among activities by defining the source activities that produce the inputs and the destination activities that receive the outputs. The standard specifies activities that must be performed and their inter-relationships; it does not specify complete acceptance criteria for determining whether the activities themselves are properly designed. Therefore, the standard should be used in conjunction with guidance from other appropriate regulatory guides, standards, and software engineering literature. IEEE Std 1074-1995 can be used as a basis for developing specific software life cycle processes that are consistent with regulatory requirements, as applied to software, for controlling and coordinating the design of safety system software.

Software development processes are intimately related to system development processes. In the system design phase, system safety requirements are allocated to hardware, software, and human elements. In the system integration and testing phases, these elements are combined and tested. Consequently, a standard for software development processes is intimately related to system-level standards, such as IEEE Std 7-4.3.2-1993, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," which is endorsed by Revision 1 of Regulatory Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants." IEEE Std 1074-1995 describes a complete set of software life cycle processes; however, its system-level view is a generic view from a software perspective. To employ IEEE Std 1074-1995 for developing safety system software, the system-level activities described in IEEE Std 1074-1995 must be addressed within the context provided by regulation and by nuclear industry

standards. Examples of system-level issues from this context are the need for software safety analyses as part of system safety evaluation and the need for determining the acceptability of pre-existing software for use in safety systems. Information on software safety activities and software life cycle activities in general can be found in Revision 1 of Regulatory Guide 1.152; NUREG/CR-6101, "Software Reliability and Safety in Nuclear Reactor Protection Systems"⁵ (November 1993); and NUREG/CR-6263, "High Integrity Software for Nuclear Power Plants: Candidate Guidelines, Technical Basis and Research Needs"⁵ (June 1995). The second area, the acceptability of pre-existing software, is particularly important in the nuclear context. Guidance on this subject is in Revision 1 of Regulatory Guide 1.152.

C. REGULATORY POSITION

The requirements⁶ contained in IEEE Std 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes,"³ provide an approach acceptable to the NRC staff for meeting the requirements of 10 CFR Part 50 and the guidance in Revision 1 of Regulatory Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," as they apply to development processes for safety system software, subject to the provisions listed below. The appendices to IEEE Std 1074-1995 are not endorsed by this regulatory guide.

To meet the requirements of 10 CFR 50.55a(h) and Appendix A to 10 CFR Part 50 as ensured by complying with the criteria of Appendix B applied to the development processes for safety system software, the following provisions are necessary and will be considered by the NRC staff in the review of applicant submittals. (In this Regulatory Position, the cited criteria are in Appendix B to 10 CFR Part 50 unless otherwise noted.)

1. Because IEEE Std 1074-1995 was not written specifically for nuclear safety, the following clarifications apply to the standard.

⁵Copies are available at current rates from the U.S. Government Printing Office, P.O. Box 37082, Washington, DC 20402-9328 (telephone (202)512-2249); or from the National Technical Information Service by writing NTIS at 5285 Port Royal Road, Springfield, VA 22161. Copies are available for inspection or copying for a fee from the NRC Public Document Room at 2120 L Street NW., Washington, DC; the PDR's mailing address is Mail Stop LL-6, Washington, DC 20555; telephone (202)634-3273; fax (202)634-3343.

⁶In 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.

1.1 Criterion III, "Design Control," requires measures to ensure that applicable regulatory requirements and the design basis for those structures, systems, and components to which Appendix B applies are correctly translated into specifications, drawings, procedures, and instructions. The descriptions of input information, life cycle activity, and output information that are required by IEEE Std 1074-1995 must identify applicable regulatory requirements, design bases, and related guidance.

1.2 Various statements in the standard imply or state that life cycle activities should be consistent with budget and schedule or that contingency actions may be taken to meet schedule or budget (paragraphs 3.2.3 and 3.2.4 of IEEE Std 1074-1995). All such activities and contingency actions must be consistent with and justifiable with 10 CFR 50.57(a)(3), which requires 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.

1.3 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. If pre-existing software (i.e., reusable software or commercial off-the-shelf software) is incorporated into a safety system developed under the method described by this regulatory guide, an acceptance process must be included at an appropriate point in the life cycle model to establish the suitability of the pre-existing software for its intended use. The acceptance process, its inputs, outputs, activities, pre-conditions, and post-conditions, must meet the applicable regulatory requirements and design bases for the safety system.

2. Criterion II, "Quality Assurance Program," requires all activities affecting quality to be accomplished under suitably controlled conditions. Section

1.5.1, "Applicability," of IEEE Std 1074-1995 permits elimination of some life cycle activities, although compliance with the standard may not then be claimed. According to this regulatory guide, compliance with IEEE Std 1074-1995 means that all mandatory activities are performed, that the requirements described as 'shall' are met, and that all the inputs, outputs, activities, pre-conditions, and post-conditions mentioned by IEEE Std 1074-1995 are described or accounted for in the applicant's life cycle model. IEEE Std 1074-1995 is an organizing standard that ensures that activities deemed important to software quality are performed and related properly to each other; it does not provide detailed information regarding the implementation of specific life cycle activities.

3. Criterion III, "Design Control," requires measures to ensure that applicable regulatory requirements and the design basis are correctly translated into specifications, drawings, procedures, and instructions. To ensure that safety system software development is consistent with the defined system safety analyses, additional activities beyond those specified in IEEE Std 1074-1995 are necessary. Planned and documented software safety analysis activities should be conducted for each phase of the software development life cycle. Therefore, these analyses should be identified in the applicant's life cycle model, including the following inputs, activity description, and outputs.

3.1 Input Information

- Regulatory requirements and guidance,
- Information reported for the system safety analysis,
- Information from previous phases for the software safety analysis,
- The design information from previous and current system and software phase activities.

3.2 Description

The analyses must ensure that:

- System safety requirements have been correctly addressed,
- No new hazards have been introduced,
- Software elements that can affect safety are identified,

- There is evidence that other software elements do not affect safety, and
- Safety problems and resolutions identified in these analyses are documented.

These activities must be conducted according to a Software Safety Plan addressing the organization to perform the analyses, the responsibilities of its safety officer, the management of the software safety activities, and the analyses to be performed for each phase to address hazards and abnormal conditions and events.

3.3 Output Information

Information for the current phase activities is reported in the software safety analysis. This information should be used for the design activities of the current life cycle phase, subsequent software safety analysis activities, the software configuration management process, and the verification and validation process.

4. Criterion XV, "Nonconforming Materials, Parts, or Components," requires measures to be established to control materials, parts, or components that do not conform to requirements in order to prevent their inadvertent use or installation. The following clarifications should be made to IEEE Std 1074-1995 with respect to the installation and operation of new or modified safety system software.

4.1 Temporary "Work-Around"

In its overview discussion of the "Installation Process," section 6.1.1 of IEEE Std 1074-1995 states: "If a problem arises, it must be identified and reported; if necessary and possible, a temporary 'work-around' may be applied." For the purposes of this regulatory guide, the term 'work-around' is defined as follows.

A temporary change, to either the software or its configuration, that is made for the purpose of allowing the continuation of installation activities and testing of parts of the software that are unaffected by the temporary change.

4.2 Installation

Installation of new or modified safety system software may only be performed when all functions affected by the software have been declared inoperable according to the plant technical specifications. When software is involved, particularly for distributed software architectures, the determination of affected functions can depend on extremely subtle considerations. An example would be two programs related to each other only through use of a single data item, which might not be evident from the examination of architecture diagrams. As a minimum, all functions performed, in part, by a given software executable should be declared inoperable if the software executable, its configuration, or its operating platform is to be altered; interconnections of all types with other software, hardware, or human elements should also be examined. Any work-arounds employed during installation must be accompanied by a disposition plan, rework procedures that conform to configuration control, verification and validation procedures agreed to under the licensing basis, and a resolution schedule. Before affected functions may be declared operable, the currently approved software, under the control of configuration management, must be installed according to the procedures specified in the installation process. This ensures that the intended software is installed and that any work-arounds employed during the installation activities are removed.

4.3 Operation

Section 6.2.3, "Operate the System," of IEEE Std 1074-1995 requires the identification and reporting of anomalies as well as invocation of the verification and validation (V&V) process and the software configuration management process. Section 6.3, "Maintenance Process," requires the software life cycle to be "remapped and executed, thereby treating the Maintenance Process as iterations of development." This process will produce revisions to software executables and configurations that may then be installed according to the installation process. Maintenance activities must conform to the configuration control and V&V procedures agreed to under the licensing basis.

5. Criterion V, "Instructions, Procedures, and Drawings," requires that activities affecting quality be prescribed by, and accomplished in accordance with, documented instructions, procedures, or drawings. Section 6.1.5.2 of IEEE Std 1074-1995 permits customer tailoring in the 'Install Software' activity. Any tailoring of packaged software or data in the data base at installation must be consistent with the packaged installation planned information of IEEE Std 1074-1995. Criterion III, "Design Control," requires design changes to be subject to design control measures commensurate with those applied to the original design. Tailoring that constitutes design changes, including configurations not part of the original system design, is not permitted unless such tailoring is subject to the full range of design and quality assurance measures applicable to the development of safety system software.
6. Various sections of IEEE Std 1074-1995 reference industry codes and standards. These referenced standards should be treated individually. If a referenced standard has been incorporated separately into the NRC's regulations, licensees and applicants must comply with that standard as set forth in the 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 that 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, 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 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 as computers and software replace 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 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 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

¹Copies 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.

Safety-Critical Software" (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 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 for design and manufacturing processes for hardware components.

The use of a planned and well-defined software life cycle process is important to software quality because the controlled use of such a process ensures that necessary activities are performed in a coordinated fashion and that interfaces between activities are properly implemented. The need for a controlled process that accounts for design interfaces and coordination among participating design organizations is stated in Appendix B to 10 CFR Part 50. Various life cycle process models have been proposed for software development, and there is a core set of activities in all of these processes. NUREG/CR-6101 presents a detailed discussion of software development activities and their associated design outputs, adjusted for the context of nuclear safety system software. The addition of software safety analyses is an example of this adjustment. NUREG/CR-6263 also describes these basic activities in its discussion of system context and the framework for software development and assurance. The preponderance of evidence indicates that a consistent and well-defined software development life cycle process is sufficiently important to safety system software quality that general knowledge and consensus on an acceptable method for developing such models is an appropriate subject for staff review.

²Copies are available at current rates from the U.S. Government Printing Office, P.O. Box 37082, Washington, DC 20402-9328 (telephone (202)512-2249); or from the National Technical Information Service by writing NTIS at 5285 Port Royal Road, Springfield, VA 22161. Copies are available for inspection or copying for a fee from the NRC Public Document Room at 2120 L Street NW., Washington, DC; the PDR's mailing address is Mail Stop LL-6, Washington, DC 20555; telephone (202)634-3273; fax (202)634-3343.

2. ALTERNATIVE APPROACHES

Based on the studies cited 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 advantage 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 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 it is 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 would 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
 - Addresses 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. Implementation of these systems must be consistent with the NRC'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 on 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.



Federal Recycling Program

¹Copies may be purchased at current rates from the U.S. Government Printing Office, P.O. Box 37082, Washington, DC 20402-9328 (telephone (202)512-2249); or from the National Technical Information Service by writing NTIS at 5285 Port Royal Road, Springfield, VA 22161. Copies are available for inspection or copying for a fee from the NRC Public Document Room at 2120 L Street NW., Washington, DC; the PDR's mailing address is Mail Stop LL-6, Washington, DC 20555; telephone (202)634-3273; fax (202)634-3343.

²Single 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