U.S. NUCLEAR REGULATORY COMMISSION

July 2013
Revision 1

REGULATORY GUIDE

OFFICE OF NUCLEAR REGULATORY RESEARCH

Technical Lead
Karl Sturzebecher

REGULATORY GUIDE 1.173

(Draft was issued as DG-1210, dated August 2012)

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

A. INTRODUCTION

Purpose

This regulatory guide (RG) describes a method that the staff of the U.S. Nuclear Regulatory Commission (NRC) considers acceptable for use in complying with NRC regulations on the development of software life cycle processes for digital computer software used in the safety systems of nuclear power plants.

Applicable Rules and Regulations

The regulatory framework the NRC has established for nuclear power plants consists of a number of regulations and supporting guidelines applicable to the development of software life-cycle processes for digital computer software. In Title 10, of the *Code of Federal Regulations*, Part 50, "Domestic Licensing of Production and Utilization Facilities," (Ref. 1), paragraph 55a(a)(1) requires, in part 1 that systems and components be designed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed. Also in 10 CFR Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants," the General Design Criterion (GDC) 1, "Quality Standards and Records," requires, in part, that quality standards be established and implemented to provide adequate assurance that systems and components important to safety will satisfactorily perform their safety functions. Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," of 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, in addition to the systems and components that directly prevent or mitigate the consequences of postulated accidents, the Appendix B criteria also apply to all activities that affect the safety-related functions of such structures, systems, and components, including designing, purchasing, installing, inspecting, testing, operating, maintaining, or modifying.

In 10 CFR 50.55a(a)(1), the NRC requires, in part, that systems and components be designed, fabricated, erected, tested, and inspected to quality standards commensurate with the importance of the

---

Written suggestions regarding this guide or development of new guides may be submitted through the NRC's public Web site under the Regulatory Guides document collection of the NRC Library at http://www.nrc.gov/reading-rm/doc-collections/reg-guides/contactus.html.

Electronic copies of this guide and other recently issued guides are available through the NRC's public Web site under the Regulatory Guides document collection of the NRC Library at http://www.nrc.gov/reading-rm/doc-collections/ and through the NRC's Agencywide Documents Access and Management System (ADAMS) at http://www.nrc.gov/reading-rm/adams.html, under Accession No. ML13009A190. The regulatory analysis may be found in ADAMS under Accession No. ML103120737 and the staff responses to public comments received on DG-1210 may be found in ADAMS under Accession No. ML13009A055.

safety function to be performed. The regulations in 10 CFR 50.55a(h)(1), the NRC requires that reactor protection and safety systems satisfy the criteria in Institute of Electrical and Electronics Engineers (IEEE) Standard (Std.) 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generation Stations," issued 1991 (including a correction sheet dated January 30, 1995) (Ref. 2), or the requirements in IEEE Std. 279, "Criteria for Protection Systems for Nuclear Power Generating Stations," issued 1971 (Ref. 3). These criteria shall be part of the evaluation of the recognized quality codes and standards selected for their applicability, adequacy and sufficiency and shall be supplemented or modified as needed to assure the production of a quality product that will perform the required safety function. The guidance on the safety systems equipment employing digital computer software or firmware requires quality standards in the use of the project life cycle process.

This RG endorses the guidance in IEEE Std. 1074-2006, "IEEE Standard for Developing a Software Project Life Cycle Process," issued 2006 (Ref. 4), with the exceptions stated in the regulatory positions, as a method acceptable to the NRC staff for complying with NRC regulations to promote high functional reliability and design quality in software used in safety systems.[1] In particular, the method is consistent with the previously cited GDC in Appendix A to 10 CFR Part 50 and the criteria for quality assurance programs in Appendix B to 10 CFR Part 50 as they apply to software development processes. The criteria of Appendices A and B to 10 CFR Part 50 apply to systems and related quality assurance processes, and the requirements also extend to the software elements if those systems include software.

Purpose of Regulatory Guides

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

Paperwork Reduction Act

This RG contains information collection requirements covered by 10 CFR Part 50 and 10 CFR Part 52 that the Office of Management and Budget (OMB) approved under OMB control numbers 3150-0011 and 3150-0151, respectively. The NRC may neither conduct nor sponsor, and a person is not required to respond to, an information collection request or requirement unless the requesting document displays a currently valid OMB control number.

1 The term "safety systems" is synonymous with "safety-related systems." The scope of the GDC includes systems, structures, and components "important to safety." However, the scope of this regulatory guide is limited to "safety systems," which are a subset of "systems important to safety." Although not specifically scoped to include non-safety-related but "important to safety systems" this regulatory guide provides methods that the staff finds appropriate for the design, development and implementation of all important to safety systems. The NRC may apply this guidance in licensing reviews of non-safety but important to safety digital software and may tailor it to account for the safety significance of the system software.

B. DISCUSSION

Background

The use of industry consensus standards is part of an overall approach to meet the requirements in 10 CFR Part 50 when developing safety systems for nuclear power plants. A licensee's compliance with these standards does not guarantee that it will meet regulatory requirements. However, the licensee's compliance with these standards does ensure that it will incorporate practices accepted within various technical communities 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 the development of such systems.

This RG refers to software incorporated into the instrumentation and control systems covered by Appendix B to 10 CFR Part 50 as "safety system software." For safety system software, the development of 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. A number of consensus standards provide guidance on implementing currently accepted approaches to specific software engineering activities, such as software requirements specification, software testing and documentation, software verification, validation, reviews and audits, or software configuration management. A carefully planned and controlled software development effort should incorporate these specific activities into an orderly process within the software life cycle, including pre-software and post-software development processes. This RG addresses the subject of designing software life-cycle processes appropriate for the development of safety system software.

The following criteria in Appendix B to 10 CFR Part 50 contain requirements closely related to software life-cycle activities. These listed criteria are only part of and not the entire requirement:

- Criterion I, "Organization," requires, in part, the establishment and execution of a quality assurance program.

- Criterion II, "Quality Assurance Program," requires, in part, that activities affecting quality are accomplished under suitably controlled conditions that take into account the need for special controls and processes to attain the required quality.

- Criterion III, "Design Control," requires, in part, that measures be established for the identification and control of design interfaces and for coordination among participating design organizations.

- Criterion VI, "Document Control," requires, in part, that all documents that prescribe activities affecting quality, such as instructions, procedures, and drawings, be subject to controls that ensure that authorized personnel review documents, including changes, for adequacy and approve them for release.

- Criterion VII, "Control of Purchased Material, Equipment, and Services," requires, in part, that measures are established to ensure that purchased material, equipment, and services, whether purchased directly or through contractors and subcontractors, conforms to the procurement documents.

- Criterion XV, "Nonconforming Materials, Parts, or Components," requires, in part, that measures are established to control materials, parts, or components that do not conform to requirements in order to prevent their inadvertent use or installation.

- Criterion XVII, "Quality Assurance Records," requires, in part, that sufficient records be maintained so that data closely related to activities affecting quality, such as the qualification of personnel, procedures, and equipment, are identifiable and retrievable.

Description of Change

The original version of this RG endorsed IEEE Std. 1074-1995. With the refocus on the software project life-cycle planning process, which is the initiation task in devising a software project life cycle model, the IEEE Std. 1074-2006 version realigns most of the original 1995 process activities into activity groups under Annex A. These 2006 activities include new topics such as A.1.1.5.1, "Determine Security Objectives." In response to this new activity, the RG 1.173 has also added a new Subsection Part C, 1, d, "Secure Analysis," and acknowledges that planning for security and confirming the security accreditations is necessary and part of a secure analysis.

However, to meet criteria of IEEE Std. 603-1991 and 10 CFR 50, the development of digital safety system software requires a secure development and operational environment (SDOE) be provided, RG 1.152 provides specific guidance concerning the establishment of SDOEs. For licensees that choose to provide, as part of their license submittal, descriptions of cyber-security design features intended to address the guidance of RG 5.71, the extent of the staff's review of these features is limited to ensuring that these features do not adversely affect or degrade the system's reliability or its capability to perform its safety function.

Applicants and licensees should be aware that other NRC requirements and guidance may lead to specific cyber security controls during the software development process and/or the inclusion of security features in or around digital safety systems; however, a licensee's adherence to the provisions of 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks," (Ref. 7) will be evaluated per regulatory programs specific to that regulation and in accordance with the applicant's NRC-approved cyber security plan. IEEE Std. 1074-2006 is not endorsed in this RG as being appropriate for compliance with 10 CFR 73.54 in this RG.

There are other activities that have been added to the new IEEE Std. 1074-2006 version such as: A.1.2.9 "Plan Release Management," A.1.3.6 "Close Project," A.2.3 "Software Importation Activity Group," and A.3.3.4 "Manage Software Release," which are all supported activities to this RG 1.173.

Other changes to this RG include IEEE Std. 1074-1995, Clause 3.3, "Software Quality Management Process" which was dropped from the 2006 version. The applicant and licensee should refer to RG 1.28 "Quality Assurance Program Criteria" (Ref. 8) for more information on this topic. The other process section, "Verification and Validation Process," was removed from the IEEE Std. 1074-1995 version and transformed to a peer and/or technical review set of activities in the new IEEE Std. 1074-2006, Annex Section A.5.1, called "Evaluation Activity Group." In any lifecycle frame the developer should always provide review, audit, and test milestones for the software project; however, this does not release the applicant or licensee from performing a formal software V&V, technical reviews, or audits to meet general quality and reliability requirements in GDC 1 or GDC 21, "Protection System Reliability and Testability," of Appendix A to 10 CFR Part 50, as well as Criterion II, III, XI, and XVIII of Appendix B. Additional information and guidance for performing a software V&V can be found in RG 1.168 "Verification, Validation, Reviews and Audits for Digital Computers Software Used in Safety Systems of Nuclear Power Plants" (Ref. 9).

This revision to RG 1.173 has added a clarification statement to highlight one of the existing planning activities in IEEE Std. 1074-2006, Annex Section A.1.2.3. This statement is found under Part C.4.d., "System Transitions," and states all changes to safety systems must be evaluated using the criteria specified in 10 CFR 50.59. If the change is outside the scope of 10 CFR 50.59, then it must be submitted for review as a licensing amendment request.

Related Guidance

In terms of inputs, development, verification or control processes, and outputs, IEEE Std. 1074 2006 describes a set of processes and constituent activities that are commonly accepted as comprising a controlled and well-coordinated software project life cycle process. It promulgates interrelationships among the life cycle activity groups by the entry input and output information, and the source and destination activities. The standard specifies mapping on to an appropriate software project life cycle model. 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 RGs, standards, and software engineering literature. IEEE Std. 1074-2006 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. The system design phase allocates system safety requirements to hardware, software, and human elements. The system integration and testing phases combine and test these elements. Consequently, a standard for software development processes is inherently related to system-level standards, such as IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," issued 2003 (Ref. 10), which RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants" (Ref. 11), endorsed in January, 2006. IEEE Std. 1074-2006 describes a complete set of software life-cycle processes; however, its system-level view is a generic view from a software perspective. To use IEEE Std. 1074-2006 for developing safety system software, the system-level activities described in IEEE Std. 1074-2006 should be addressed within the context provided by regulation and by nuclear industry standards.

Examples of system-level issues from this context are (1) the need for software safety analyses as part of system safety evaluation and (2) the need for determining the acceptability of preexisting (pre-developed) software for use in safety systems. RG 1.152; NUREG/CR-6101, "Software Reliability and Safety in Nuclear Reactor Protection Systems," issued November 1993 (Ref. 12); and NUREG/CR-6263, "High Integrity Software for Nuclear Power Plants: Candidate Guidelines, Technical Basis, and Research Needs," issued June 1995 (Ref. 13), contain general information on software safety activities and software life-cycle activities. The second area, the acceptability of preexisting (pre-developed) software, is particularly important in the nuclear context, and further guidance can be found in RG 1.152.

The software development process has several supporting RGs to promote high functional reliability and design quality in the software used in safety systems. These guides include the following:

a. RG 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,"

b. RG 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Ref. 14),

c. RG 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Ref. 15),

d. RG 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Ref. 16), and

e. RG 1.172, "Software Requirement Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Ref. 17).

This RG is based on standards and describes methods acceptable for any safety system software and it discusses the required life cycle activities. The applicant or licensee determines how the required activities will be implemented.

Harmonization with International Standards

The International Atomic Energy Agency (IAEA) has established a series of safety guides and standards constituting a high level of safety for protecting people and the environment. IAEA safety guides are international standards to help users striving to achieve high levels of safety. Pertinent to this RG, IAEA Safety Guide NS-G-1.1, "Software for Computer Based Systems Important to Safety in Nuclear Power Plants" issued September 2000 (Ref. 18) discusses the importance of project plans for computer software used in safety related systems. This RG incorporates similar project recommendations and is consistent with the basic principles provided in IAEA Safety Guide NS-G-1.1.

Documents Discussed in Staff Regulatory Guidance

This RG endorses, in part, the use of one or more codes or standards developed by external organizations, and other third party guidance documents. These codes, standards and third party guidance documents may contain references to other codes, standards or third party guidance documents ("secondary references"). If a secondary reference has itself been incorporated by reference into NRC regulations as a requirement, then licensees and applicants must comply with that standard as set forth in the regulation. If the secondary reference has been endorsed in a RG as an acceptable approach for meeting an NRC requirement, then the standard constitutes a method acceptable to the NRC staff for meeting that regulatory requirement as described in the specific RG. If the secondary reference has neither been incorporated by reference into NRC regulations nor endorsed in a RG, then the secondary reference is neither a legally-binding requirement nor a "generic" NRC approved acceptable approach for meeting an NRC requirement. However, licensees and applicants may consider and use the information in the secondary reference, if appropriately justified, consistent with current regulatory practice, and consistent with applicable NRC requirements.

C. STAFF REGULATORY GUIDANCE

IEEE Std. 1074-2006 provides an approach that the NRC staff considers acceptable for meeting the requirements in 10 CFR Part 50 and the guidance in RG 1.152, as they apply to development processes for safety system software with the exceptions and additions listed in these regulatory positions. In this section of the guide, the cited criterion refers to Appendix A or B to 10 CFR Part 50 unless otherwise noted. The NRC staff will consider these exceptions and additions in its review of submittals from applicants and licensees.

1. Clarifications

Because IEEE Std. 1074-2006 was not written specifically for nuclear safety, the following clarifications apply to the standard:

a. Identification of Regulatory Requirements. Criterion III of Appendix B to 10 CFR Part 50 requires, in part, the establishment of measures to ensure that applicable regulatory requirements and the design bases 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. 1074-2006 should identify applicable regulatory requirements, design bases, and related guidance.

b. Consistency. Various statements in IEEE Std. 1074-2006, such as: Section A.1.3.1 "Manage Risk" imply or state that life-cycle activities should be consistent with cost and schedule or that contingency actions may be taken to meet schedule or cost. All such activities and contingency actions should be consistent with, and justifiable in terms of, Criterion I of Appendix B, which requires that there be sufficient authority and organizational freedom, including sufficient independence from cost and schedule when those actions opposed to safety software quality are considered. The applicant or licensee is not relieved of the responsibility for ensuring reasonable assurance that activities selected can be conducted without endangering public health and safety.

c. Commercial Software. In reference to all activities under Section A.2.2.3 "Allocate System Requirements" to IEEE 1074-2006 the Criterion III of Appendix B to 10 CFR Part 50 requires, in part, that measures be established for the selection and review for suitability of the application of materials, parts, equipment, and processes that are essential to the safety-related functions of the structures, systems, and components. Criterion VII requires, in part, that measures be established to ensure that purchased material, whether purchased directly or through contractors and subcontractors, conforms to the procurement documents. If preexisting (pre-developed) software (i.e., reusable software or commercial off-the-shelf software) is incorporated into a safety system developed under the method described by this RG, an acceptance process should be included at an appropriate point in the life-cycle model to establish the suitability of the preexisting (pre-developed) software for its intended use. The acceptance process, its inputs, outputs, activities, preconditions, and postconditions should meet the applicable regulatory requirements and design bases for the safety system. RG 1.152 provides information on the acceptance of preexisting (pre-developed) software. Additional detailed information on acceptance processes appear in Electric Power Research Institute (EPRI) TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," issued October 1996 (Ref. 19), which was accepted by a NRC issued safety evaluation report (SER) dated July 17, 1997.

d. Secure Analysis. The NRC takes exception to the IEEE Std. 1074-2006's directions for appropriate security assurance level in Section A.1.1.5 "Determine Security Objectives (Required)." The planning activity is necessary and the applicant or licensee should refer to the following primary security objectives: (i) secure software development environment, and (ii) cyber security. Guidance for secure software development is available in RG 1.152, whereas guidance for cyber security is available in RG 5.71, "Cyber Security Programs for Nuclear Facilities" (Ref. 20).

e. Definitions. The following definitions are used in this RG:

(1) Accident. An unplanned event or series of events that result in death, injury, illness, environmental damage, or damage to, or loss of, equipment or property.

(2) Hazard. A condition that is a prerequisite to an accident.

2. Compliance with IEEE Std. 1074-2006

Criterion II of Appendix B to 10 CFR Part 50 requires all activities affecting quality to be accomplished under suitably controlled conditions. Subclause 1.5, "Conformance," of IEEE Std. 1074-2006 permits the elimination of some life-cycle activities, although compliance with the standard may not then be claimed. The NRC Staff position is that compliance with IEEE Std. 1074-2006 means that all mandatory activities are performed; the requirements described as "shall" are met; and all the inputs, outputs, activities, preconditions, and postconditions mentioned by IEEE Std. 1074-2006 are described or accounted for in the licensee's or applicant's life-cycle model. IEEE Std. 1074-2006 is an organizing standard that ensures that activities deemed important to software quality are performed and are related properly to one another; it does not provide detailed information on the implementation of specific life-cycle activities.

3. Software Safety Analyses

Criterion III of Appendix B to 10 CFR Part 50 requires, in part, that measures be established to assure 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, an additional activity group, "Software Safety Analysis Activity Group," is necessary. This activity group will include additional activities beyond those specified in IEEE Std. 1074-2006.

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 licensee's or applicant's life-cycle model, including the following input information, activity descriptions, and output information:

a. Input Information. Input information necessary to support software safety analyses includes (1) regulatory requirements and guidance, (2) system safety analysis information, (3) information from previous phases for the software safety analysis, and (4) design information from previous and current system and software phase activities.

b. Activity Description. The analyses should ensure that (1) system safety requirements have been correctly addressed, (2) no new hazards have been introduced, (3) software elements that can affect safety are identified, (4) there is evidence that other software elements do not affect safety, and (5) safety problems and resolutions identified in these analyses are documented.

These activities should be conducted according to a software safety plan that addresses 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.

c. Output Information. The software safety analysis reports the information for the current phase activities. The licensee or applicant should use this information 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 processes.

4. New or Modified Safety System Software

Criterion XV of Appendix B to 10 CFR Part 50 requires measures to be established to control materials, parts, or components that do not conform to requirements in an effort to prevent their inadvertent use or installation. The following clarifications should be made to IEEE Std. 1074-2006 with respect to the installation and operation of new or modified safety system software:

a. Temporary Work-Around. In its overview discussion of the installation process, Section A.4.1 of Annex A to IEEE Std. 1074-2006 states, "If a problem arises, it shall be identified and reported. If necessary, and possible, a temporary work-around may be applied." For the purposes of this RG, the term "work-around" is defined as a temporary change to either the software or its configuration that is made for the purpose of allowing the continuation of the installation activities and testing of parts of the software that are unaffected by the temporary change. A temporary work-around is not permitted in any safety system unless all software changes are performed in accordance with the software configuration controls and the changed software is checked in an off-line mode prior to installation.

b. Installation. Installation of new or modified safety system software may be performed only when all functions affected by the software have been declared inoperable in accordance with the plant technical specifications. When software is involved, particularly for distributed software architectures, the determination of affected functions can depend on extremely subtle considerations. For example, two programs related to each other only through the use of a single data item 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. All interfacing / interconnected systems must be also taken out of service and declared inoperable. A disposition plan, rework procedures that conform to configuration control and verification and validation procedures agreed to under the licensing basis, and a resolution schedule should accompany any work-arounds used during installation (Section A.4.1.2 of IEEE Std. 1074-2006). Before affected functions may be declared operable (Section A.4.1.3 of IEEE Std. 1074-2006), the currently approved software, under the control of configuration management, should 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.

c. Operation. Section A.4.2.1, "Operate the System," of Annex A to IEEE Std. 1074-2006 requires the identification and reporting of anomalies, the conduct of reviews, and the performance of configuration control. Section A.4.3, "Maintenance Activity Group," requires the software life cycle to be "remapped and executed, thereby treating the Maintenance Activity Group 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 should conform to the configuration control and verification and validation procedures agreed to under the licensing basis.

d. System Transitions. The discussion in Section A.1.2.3, "Plan System Transition," of Annex A to IEEE Std. 1074-2006 states that it is applicable only when an existing system (automated or manual) is being replaced with a new or revised system. However, all changes to safety systems must be evaluated using the criteria specified in 10 CFR 50.59. If the change is outside the scope of 10 CFR 50.59 then it must be submitted for review as a licensing amendment request.

5. Tailoring Software

Criterion V, "Instructions, Procedures, and Drawings," of Appendix B to 10 CFR Part 50 requires, in part, that activities affecting quality be prescribed by, and accomplished, in accordance with documented instructions, procedures, or drawings. Section A.4.1.2 of Annex A to IEEE Std. 1074-2006 permits data customer tailoring in the install software activity. Any tailoring of packaged software or data in the database at installation should be consistent with the packaged installation planned information of IEEE Std. 1074-2006. Criterion III requires, in part, that design changes 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. Annexes

IEEE Std. 1074-2006 contains the following six annexes (only the first annex is normative). These annexes are listed here as sources of information; they have not received regulatory endorsement unless otherwise noted:

(1) Annex A describes the detailed life-cycle activities that should be followed to conform to the standard. The annex provides normative guidance that enables effective application of the standard; therefore, the NRC staff endorses this annex with clarifications discussed in Part C of this RG.

(2) Annex B provides a mapping example that demonstrates the mapping process presented in the body of the standard (Clause 4) without constraining the user to any specific methodologies or tools. Although this example provides the licensee with good advice, Annex B is not necessary to conform to the standard; therefore, the NRC staff does not endorse this annex.

(3) Annex C gives a mapping template that may be used to assist project managers in identifying project-critical deliverables and in ensuring their completion as needed. Although this template provides the licensee with good advice, Annex C is not necessary to conform to the standard; therefore, the NRC staff does not endorse this annex.

(4) Annex D gives examples of software life-cycle models that the licensee may use to conform to the standard. The NRC staff does not endorse this annex because it provides examples only and contains no guidance.

(5) Annex E gives a glossary of terms that are used in the standard. The NRC staff finds this information useful, but does not endorse this annex without further review.

(6) Annex F gives a bibliography of other standards that IEEE Std. 1074-2006 references. The paragraph titled "Documents Discussed in Staff Regulatory Guidance," in Section B of this RG discusses the treatment of these standards.

D. IMPLEMENTATION

The purpose of this section is to provide information on how applicants and licensees[2] may use this guide and information about the NRC's plans for using this RG. In addition, it describes how the staff complies with 10 CFR 50.109, "Backfitting" and any applicable finality provisions in 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants."

Use by Applicants and Licensees

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

Licensees may use the information in this RG for actions that do not require NRC review and approval, such as changes to a facility design under 10 CFR 50.59, "Changes, Tests, and Experiments." Licensees may use the information in this RG or applicable parts to resolve regulatory or inspection issues.

This RG is not being imposed upon current licensees and may be voluntarily used by existing licensees. Additionally, an existing applicant may be required to adhere to new rules, orders, or guidance if 10 CFR 50.109(a)(3) applies.

If a licensee believes that the NRC either is using this RG or requesting or requiring the licensee to implement the methods or processes in this RG in a manner inconsistent with the discussion in this implementation section, then the licensee may file a backfit appeal with the NRC in accordance with the guidance in NUREG-1409, "Backfitting Guidelines," (Ref. 21) and the NRC Management Directive 8.4, "Management of Facility-Specific Backfitting and Information Collection" (Ref. 22).

Use by NRC Staff

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

---

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

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

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

The staff does not intend or approve any imposition or backfitting of the guidance in this RG. The staff does not expect any existing licensee to use or commit to using the guidance in this RG, unless the licensee makes a change to its licensing basis. The staff does not expect or plan to request licensees to voluntarily adopt this RG to resolve a generic regulatory issue. The staff does not expect or plan to initiate NRC regulatory action that would require the use of this RG. Examples of such unplanned NRC regulatory actions include issuance of an order requiring the use of the RG, requests for information under 10 CFR 50.54(f) as to whether a licensee intends to commit to use of this RG, generic communication, or promulgation of a rule requiring the use of this RG without further backfit consideration.

REFERENCES[4]

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

2. Institute of Electrical and Electronic Engineers (IEEE), Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Piscataway, NJ, 1991 (including a correction sheet dated January 30, 1995).[5]

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

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

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

6. CFR, "Licenses, Certifications, and Approvals for Nuclear Power Plants," Part 52, Chapter 1, Title 10, "Energy."

7. CFR, "Protection of Digital Computer and Communication Systems and Networks," Part 73, Chapter 1, Title 10, "Energy."

8. NRC, Regulatory Guide (RG) 1.28, "Quality Assurance Program Criteria," Washington, D.C.

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

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

11. NRC, RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Washington, DC.

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

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

---

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

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

14. NRC, RG 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Washington, DC.

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

16. NRC, RG 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Washington, DC.

17. NRC, RG 1.172, "Software Requirement Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Washington, DC.

18. International Atomic Energy Agency (IAEA) Safety Guide NS-G-1.1, "Software for Computer Based Systems Important to Safety in Nuclear Power Plants" issued September 2000.[6]

19. Electric Power Research Institute (EPRI) Topical Report TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," Palo Alto, CA, October 1996.[7] (ADAMS Accession No. ML092190664)

20. NRC, RG 5.71, "Cyber Security Programs for Nuclear Facilities," Washington, DC.

21. NRC, NUREG-1409, "Backfitting Guidelines," Washington, DC. (ADAMS Accession No. ML032230247)

22. NRC, Management Directive 8.4, "Management of Facility-Specific Backfitting and Information Collection," Washington DC. (ADAMS Accession No. ML050110156)

6 Copies of International Atomic Energy Agency (IAEA) documents may be obtained through their Web site: WWW.IAEA.Org/ or by writing the International Atomic Energy Agency P.O. Box 100 Wagramer Strasse 5, A-1400 Vienna, Austria. Telephone (+431) 2600-0, Fax (+431) 2600-7, or E-Mail at Official.Mail@IAEA.Org

7 Copies of EPRI documents may be obtained from the Electric Power Research Institute, 3420 Hillview Avenue, Palo Alto, CA 94304, telephone 650-855-2000 or online at http://my.epri.com/portal/server.pt.