U.S. NUCLEAR REGULATORY COMMISSION

July 2013
Revision 1

REGULATORY GUIDE

OFFICE OF NUCLEAR REGULATORY RESEARCH

Technical Lead
Karl Sturzebecher

REGULATORY GUIDE 1.172

(Draft was issued as RG-1209, dated August 2012)

SOFTWARE REQUIREMENT SPECIFICATIONS FOR DIGITAL COMPUTER SOFTWARE AND COMPLEX ELECTRONICS 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 software requirement specifications (SRSs) for digital computer software used in the safety systems of nuclear power plants.

Applicable Rules and Regulations

The regulatory framework that the NRC has established for nuclear power plants consists of a number of regulations and supporting guidelines applicable to the SRSs for digital computer software. Title 10, of the *Code of Federal Regulations*, Part 50, “Domestic Licensing of Production and Utilization Facilities” (10 CFR Part 50) (Ref. 1), Appendix A, “General Design Criteria for Nuclear Power Plants,” General Design Criterion (GDC) 1, requires, in part, that systems and components be designed, tested, and inspected to quality standards commensurate with the safety function to be performed, while the nuclear power unit licensee maintains, or controls the maintenance of, appropriate records on the design and testing of systems and components important to safety throughout the life of the unit. 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 must meet for systems and components that prevent or mitigate the consequences of postulated accidents. 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, including designing, purchasing, installing, inspecting, testing, operating, maintaining, or modifying, that affect the safety-related functions of such structures, systems, and components.

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 safety function to be performed. 10 CFR 50.55a(h) requires licensees to satisfy the criteria for reactor protection systems in Institute of Electrical and Electronics Engineers (IEEE) Standard (Std.) 603-1991, “IEEE Standard

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. ML13007A173. The regulatory analysis may be found in ADAMS under Accession No. ML103080966 and the staff responses to the public comments on DG-1209 may be found in ADAMS under Accession No. ML13007A160.

Criteria for Safety Systems for Nuclear Power Generating Stations," issued 1991 (including a correction sheet dated January 30, 1995) (Ref. 2), or in IEEE Std. 279-1971, "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 a quality product that will perform the required safety function. The guidance for safety system equipment employing digital computers and programs or firmware requires the use of a quality standard for the development of software and firmware requirement specifications.

This RG endorses IEEE Std. 830-1998, "IEEE Recommended Practice for Software Requirements Specifications," issued in 1998 and reaffirmed in 2009 (Ref. 4), with the exceptions stated in the regulatory positions. IEEE Std. 830-1998 describes methods that the NRC staff considers acceptable for use in complying with the NRC regulations for achieving high functional reliability and design quality in software used in safety systems.[1] In particular, the methods are consistent with the previously cited GDC and the criteria for quality assurance programs in Appendix B to 10 CFR Part 50 as they apply to the development of SRSs. The criteria of Appendix A and Appendix B to 10 CFR Part 50 apply to systems and related quality standards and quality assurance processes as well as the software elements of those systems.

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.

B. DISCUSSION

Background

The use of voluntary consensus standards, such as IEEE standards, is part of an overall approach to meeting the requirements of 10 CFR Part 50 when developing safety systems for nuclear power plants.

[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.

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.

Several criteria in Appendix A to 10 CFR Part 50 describe functions that are part of the design bases of nuclear power plants and that would be included in the SRSs of any digital computer software that is part of the basic components that perform these functions. These listed criteria include part of GDC requirements such as: GDC 1, "Quality Standards and Records," GDC 12, "Suppression of Reactor Power Oscillations," GDC 13, "Instrumentation and Control," GDC 19, "Control Room," GDC 20, "Protection System Functions," GDC 22, "Protection System Independence," GDC 23, "Protection System Failure Modes," GDC 24, "Separation of Protection and Control Systems," GDC 25, "Protection System Requirements for Reactivity Control Malfunctions," and GDC 28, "Reactivity Limits."

In addition to the criteria of Appendix A, 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." The SRS is an essential part of the record of the design of safety system software. Software requirements are associated with the system requirements allocated to software subsystems and serve as the design bases for the software under development. Therefore, SRSs are a crucial design input to the remainder of the software development process. SRSs should exhibit characteristics such as correctness and completeness that will facilitate the implementation of a carefully planned and controlled software development process. Appendix B to 10 CFR Part 50 provides quality assurance criteria that the design documentation for nuclear reactor safety systems must meet through design control measures. Criterion III, "Design Control," of Appendix B requires licensees to develop these control measures for design documentation and identification and the control of design interfaces and measures for verifying or checking the adequacy of the design.

Description of Change

The original version of this RG endorsed IEEE Std. 830-1993. There are only minor changes between IEEE Std. 830-1998 and the original 1993 version. This version of RG 1.172 endorses IEEE Std. 830-1998, specifically addresses Annex B, and corrects three other perspectives associated with the software attributes of an SRS. The updated areas are: the enhancements in "Security," the addition of "Unambiguity" and the deletion of an existing section called "Nonapplicability."

The original RG contained a section called "Nonapplicability," which has been removed from this version because of the changes in the way software is viewed and documented. All subjects associated with the development of safety systems are applicable for review and not inherently ambiguous. A new section called "Unambiguity" has been added to this RG. Unambiguity is also addressed in IEEE Std. 830-1998 and is important because of the way digital systems interact with a variety of associated software products. As full or partial digital systems are introduced into the nuclear power designs the clarity of the SRS becomes extremely important. This is also the case where associated features must be identified during the design phase as stated in RG 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," (Ref. 7).

The NRC staff recognizes that security features or mechanisms can also play a critical role in supporting software security at higher levels of assurance. IEEE Std. 830-1998 supports this by identifying security as a specific attribute and project objective found in the SRS requirements of the safety software. Subclause 5.3.6.3 of IEEE Std. 830-1998 is not endorsed in this RG as having sufficient details for protecting software. 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.

Applicants 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. 8) will be evaluated per regulatory programs specific to that regulation and in accordance with the applicant's NRC-approved cyber security plan. IEEE Std. 830-1998 is not endorsed in this RG as being appropriate for compliance with 10 CFR 73.54.

Related Guidance

IEEE Std. 830-1998, a consensus standard on software engineering, describes the current practice for writing SRSs for a wide variety of systems. While this standard is not specifically aimed at safety applications, it does, however, provide guidance on the development of SRSs that will exhibit characteristics important in the development of safety system software. This guidance is consistent with the NRC's goals of promoting high functional reliability and design quality in software used in safety systems.

Other standards that mention SRSs but do not provide detailed guidance for writing them include:

- IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," issued 2003 (Ref. 9), identifies unambiguous software requirements as a prerequisite for high-quality software development. RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants" (Ref. 10), endorses this standard.

- IEEE Std. 1012-2004, "IEEE Standard for Software Verification and Validation," issued 2004 (Ref. 11), also identifies unambiguous software requirements as a prerequisite for verification and validation. RG 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Ref. 12), endorses this standard.

- IEEE Std. 1074-2006, "IEEE Standard for Developing a Software Life Cycle Process," issued 2006 (Ref. 13), describes SRSs as an essential input at the beginning of a software development life cycle. RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Ref. 14), endorses this standard.

The correct, complete, well-written, and unambiguous software requirements are essential inputs to the main design and verification processes that the NRC considers necessary to produce safety-related software products. To assist in this effort there are other NRC documents available. (See NUREG/CR-6101, "Software Reliability and Safety in Nuclear Reactor Protection Systems," issued November 1993 (Ref. 15), and NUREG/CR-6263, "High Integrity Software for Nuclear Power Plants: Candidate Guidelines, Technical Basis, and Research Needs," issued June 1995 (Ref. 16))

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. 17),

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

d. RG 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Ref. 18), and

e. RG 1.173, "Developing Software Life-Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

This RG is based on standards and describes methods acceptable for any safety system software and discusses the required SRS 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. 19) discusses the importance of specifications for computer software used in safety related systems. This RG incorporates similar specifications recommendations and is consistent with the basic principles provided in IAEA Safety Guide NS-G-1.1.

Documents Discussed in Staff Regulatory Guidance

This regulatory guide 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 regulatory guide 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 regulatory guide. If the secondary reference has neither been incorporated by reference into NRC regulations nor endorsed in a regulatory guide, 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. 830-1998 provides an approach that the NRC staff considers acceptable for meeting the requirements in 10 CFR Part 50 on the preparation of SRSs 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.

1. Definitions

Clause 3 of IEEE Std. 830-1998 refers to IEEE Std. 610.12 1990, "IEEE Standard Glossary of Software Engineering Terminology," issued 1990 (Ref. 20), for the definitions of technical terms. These definitions are acceptable with the following clarifications and additions:

a. Baseline. Meaning (1) of "baseline" in IEEE Std. 610.12 1990 must be used in IEEE Std. 830-1998. "Formal review and agreement" is considered to mean that responsible management has reviewed and approved a baseline.

b. Interface. All four variations of the definition of "interface" in IEEE Std. 610.12 1990 must be used in IEEE Std. 830-1998, depending on the context. Meaning (1), "a shared boundary across which information is passed," is interpreted broadly, according to Criterion III of Appendix B to 10 CFR Part 50, to include design interfaces between participating design organizations.

2. Software Requirement Specifications

Clause 4.3 of IEEE Std. 830-1998 defines a set of characteristics of an acceptable SRS. The first sentence of this clause should be modified to read, "An SRS should be…." The licensee or applicant should provide the following clarifications and additional information for this set of characteristics for safety system software:

a. Traceability and Accuracy. When the licensee or applicant uses specifications or representation tools for requirements, as described in Subclauses 4.3.2.2 and 4.3.2.3 of IEEE Std. 830-1998, traceability must be maintained between these representations and the natural language descriptions of the software requirements that are derived from system requirements and system safety analyses to meet the requirements in GDC 1 of Appendix A to 10 CFR Part 50.

b. Completeness. For safety system software, the description of functional requirements should specify how functions are initiated and terminated and should specify the system status at termination. The licensee or applicant should provide the accuracy requirements, including units, error bounds, data type, and data size, for each input and output variable. The licensee or applicant should fully describe the variables that are controlled or monitored in the physical environment and should describe expressly prohibited functions.

Timing information is particularly important in specifying software requirements for safety system software. The licensee or applicant should identify the functions with timing constraints and provide criteria for each mode of operation. Timing requirements should be deterministic and specified for both normal and anticipated failure conditions.

c. Consistency. Subclause 4.3.4 of IEEE Std. 830-1998 restricts the term "consistency" to mean internal consistency, noting that an external inconsistency is actually an incorrect specification of a requirement. The NRC uses the term in this RG to mean both internal and external consistency. External consistency implies that the SRS is consistent with associated software products and system products such as safety system requirements and design. Internal consistency means that no requirement in the requirements specification conflicts with any other requirement in the specification.

d. Ranking for Importance or Stability. For safety system software, this characteristic means that software requirements important to safety must be identified as such in the SRS. Criterion 20 of Appendix A, among others, describes the function that reactor protection systems must perform. Subclause 4.3.5.2 of IEEE Std. 830-1998 suggests three degrees of necessity for requirements: (1) essential, (2) conditional, and (3) optional. As used in IEEE Std. 830-1998, the terms "conditional" and "optional" refer to requirements that are not necessary for the acceptability of the software. For safety system software, unnecessary requirements should not be imposed. There may be documented variations in essential requirements, but the SRSs need to link the variations either to site and equipment variations or to specific plant design bases and regulatory provisions.

e. Verifiability. Subclause 4.3.6 of IEEE Std. 830-1998 recommends the removal or revision of unverifiable requirements. The NRC believes that all requirements should be verifiable and should be modified or restated as necessary to allow for the verification of each one.

f. Modifiability. This term is closely related to the style (form, structure, and modularity), readability, and understandability of the SRS. With respect to these characteristics, precise definitions of technical terms should be available either in the SRS itself or in a glossary.

g. Traceability. In accordance with GDC 1 of Appendix A to 10 CFR Part 50 and as described in Subclause 4.3.8 of IEEE Std. 830-1998, each identifiable requirement in an SRS must be backward traceable to a higher level requirements specification and ultimately to the system licensing (e.g., regulatory requirements that it satisfies) and the design bases (e.g., IEEE 603-1991 Clause 4). Each identifiable requirement should be written so that it can also be forward traceable to subsequent design outputs (e.g., from SRS to software design and from software design to SRS).

Forward traceability to all documents derived from the SRS includes verification and validation materials. For example, a forward trace should exist from each requirement in the SRS to the specific inspections, analyses, or tests used to confirm that the requirement has been met.

h. Unambiguity. Subclause 4.3.2 of IEEE Std. 830-1998 states that an SRS is unambiguous if, and only if, every requirement has only one interpretation. Software requirements are generally derived from associated software products, such as safety system requirements; the combination of the SRS and such associated documents should be unambiguous.

3. Change Control in Software Requirement Specifications

Subclause 4.5(b) of IEEE Std. 830-1998 recommends that SRSs be baselined and subject to a formal process for the control of changes. Although the licensee or applicant should meet this recommendation directly through a change control procedure unique to IEEE Std. 830-1998, it may also meet it by placing the SRS under a general software configuration management program as a configuration item. In RG 1.169 The NRC stff describes software configuration management and endorses IEEE Std. 828-2005, "IEEE Standard for Software Configuration Management Plans," issued 2005 (Ref. 21).

4. Incomplete Software Requirement Specifications Entry

Any entry in an SRS that is incomplete (i.e., uses "to be determined" or "TBD"), as described in Subclause 4.3.3.1 of IEEE Std. 830-1998, must describe the applicable design bases and commitments to standards or regulations that govern the final determination of the requirement entry.

5. Design-Specific Issues

Subclause 4.7 of IEEE Std. 830-1998 recommends that design-specific issues, such as module partitioning, function allocation, and information flow, be omitted from SRSs. Subclause 4.7.1 of IEEE Std. 830-1998 states some exceptions to this policy, including reasons of security or safety. When specific design techniques or features, such as independence, separation, diversity, and defense in depth, are required by the safety system design bases or by regulation, they are an appropriate part of an SRS and should be described therein.

6. Software Attributes

Subclause 5.3.6 of IEEE Std. 830-1998 lists software attributes that can serve as requirements. The following attributes are particularly of interest for safety system software:

a. Safety. Software requirements important to safety are derived from system requirements and safety analyses and should be identified as such in the SRS. These requirements should include considerations based on the safety analysis report and on abnormal conditions and events as described in IEEE Std. 7 4.3.2 2003, which RG 1.152 endorses.

b. Secure Analysis. IEEE Std. 830-1998, Subclause 5.3.6.3 "Security" is not endorsed as having sufficient detail to define specific factors for security attributes along with requirements that are applicable to the SRS. The requirements approach to include a security attribute is useful for the licensee or applicant, however an analysis of specific factors for the SRS can be found in other available guidance. The development of digital safety system software requires a SDOE be provided. RG 1.152, "Criteria for Use of Computers in Safety Systems in Nuclear Power Plants," provides specific guidance related to the establishment of SDOE. The SDOE guidance can provide the needed attributes for the SRS.

c. Robustness. The licensee or applicant should specify the software requirements for fault tolerance and failure modes, derived either from a consideration of system-level hazards analyses or from software internals, for each operating mode. The licensee or applicant should fully specify software behavior in the presence of unexpected, incorrect, anomalous, and improper (1) input, (2) hardware behavior, or (3) software behavior, and should provide software requirements necessary to respond to both hardware and software failures, including the requirements for analysis of, and recovery from, computer system failures. The licensee or applicant should also specify the requirements for online inservice testing and diagnostics.

7. Annexes

IEEE Std. 830-1998 contains the following two informative annexes. These appendixes are listed here as sources of information; they have not received regulatory endorsement unless otherwise noted:

- Because the NRC has not endorsed Annex A, “SRS Templates,” licensees may only use it as an example. Directions on how to use an outline from Annex A, such as those directions found in Clause 5.3.7 of IEEE Std. 830-1998, may be taken as advisory only.

- Annex B, “Guidelines for Compliance with IEEE/EIA 12207.1-1997,” describes the relationship of IEEE Std. 830-1998 to IEEE/Electronic Industries Association (EIA) Std. 12207.1-1997, “Industry Implementation of International Standard ISO/IEC 12207: 1995 (ISO/IEC 12207) Standard for Information Technology-Software Life Cycle Processes-Life Cycle Data,” issued April 1998 (Ref. 22). The NRC does not endorse this annex because the agency does not endorse IEEE/EIA Std. 12207.1 1997.

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. 22) and the NRC Management Directive 8.4, “Management of Facility-Specific Backfitting and Information Collection” (Ref. 23).

[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.

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.

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. 830-1998, “IEEE Recommended Practice for Software Requirements Specifications,” Piscataway, NJ, 1998.

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. NRC, Regulatory Guide (RG) 1.170, “Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” Washington, DC.

8. CFR, “Protection of Digital Computer and Communication Systems and Networks,” Section 54, Part 73, Chapter 1, Title 10, “Energy.”

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

10. NRC, RG 1.152, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants,” NRC, Washington, DC.

11. IEEE Std. 1012-2004, “IEEE Standard for Software Verification and Validation,” Piscataway, NJ, 2004.

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

13. IEEE Std. 1074-2006, “IEEE Standard for Developing a Software Life Cycle Process,” Piscataway, NJ, 2006.

[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 1.173, “Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” Washington, DC.

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

16. NRC, NUREG/CR-6263, “High Integrity Software for Nuclear Power Plants: Candidate Guidelines, Technical Basis, and Research Needs,” June 1995. (ADAMS Accession No. ML063470590, ML063470593, and ML063600344)

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

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

19. 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, Vienna, Austria, 2000. [6]

20. IEEE Std. 610.12-1990, “IEEE Standard Glossary of Software Engineering Terminology,” Piscataway, NJ, 1990.

21. IEEE Std. 828-2005, “IEEE Standard for Software Configuration Management Plans,” Piscataway, NJ, 2005.

22. Institute of Electrical and Electronics Engineers and Electronic Industries Association (IEEE/EIA) Std. 12207.1-1997, “Industry Implementation of International Standard ISO/IEC 12207: 1995. (ISO/IEC 12207) Standard for Information Technology-Software Life Cycle Processes-Life Cycle Data,” Piscataway, NJ, April 1998.[7]

23. NRC, NUREG-1409, “Backfitting Guidelines,” Washington, DC. (ADAMS Accession No. ML032230247)

24. 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 International Organization for Standardization (ISO) documents may be obtained by writing to the International Organization for Standardization, 1, ch. de la Voie-Creuse, CP 56, CH-1211 Geneva 20, Switzerland, Telephone: +41 22 749 01 11, Fax: +41 22 749 09 47, by E-mail at sales@iso.org, or on-line at the ISO Store Web site: http://www.iso.org/iso/store.htm.