U.S. NUCLEAR REGULATORY COMMISSION

July 2013
Revision 1

REGULATORY GUIDE

OFFICE OF NUCLEAR REGULATORY RESEARCH

Technical Lead
Karl Sturzebecher

REGULATORY GUIDE 1.169

(Draft was issued as DG-1206, dated August 2012)

CONFIGURATION MANAGEMENT PLANS 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 configuration management plans 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 configuration management plans for 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, "Quality Standards and Records," requires, in part, that quality standards be established and implemented to provide adequate assurance that structures, systems, and components (SSCs) important to safety will satisfactorily perform their safety functions, and that the nuclear power unit licensee maintain and control appropriate records of the design and testing of SSCs 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 must be met by a quality assurance program for SSCs that prevent or mitigate the consequences of postulated accidents. In addition to the SSCs that directly prevent or mitigate the consequences of postulated accidents, the criteria of Appendix B also apply to all activities that affect the safety-related functions of such SSCs, including activities such as designing, purchasing, installing, inspecting, testing, operating, maintaining, and modifying. Further, Criterion III, "Design Control," of Appendix B to 10 CFR Part 50 requires, in part, that design changes "…shall be subject to design control measures commensurate with those applied to the original design..." and "The design control measures shall provide for verifying or checking the adequacy of design, … by the use of alternate or simplified calculational methods, or by the performance of a suitable testing program."

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. ML12355A642. The regulatory analysis may be found in ADAMS under Accession No. ML103200047 and the staff responses to the public comments on DG-1206 may be found in ADAMS under Accession No. ML12355A529.

safety function to be performed. The regulations in 10 CFR 50.55a(h) require that reactor protection and safety systems satisfy the criteria in Institute of Electrical and Electronics Engineers (IEEE) Standard (Std.) 603-1991, "Criteria for Safety Systems for Nuclear Power Generating Stations" (including a correction sheet dated January 30, 1995) (Ref. 2), or in IEEE Std. 279, "Criteria for Protection Systems for Nuclear Power Generating Stations" (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 on the safety systems equipment employing digital computers, and programs or firmware requires quality standards in the use of software configuration management.

This RG endorses IEEE Std. 828-2005, "IEEE Standard for Software Configuration Management Plans," issued 2005 (Ref. 4), with the exceptions stated in Section C, "Staff Regulatory Guidance." IEEE Std. 828-2005 describes methods acceptable to the NRC staff for use in complying with the NRC's regulations for quality standards that promote high functional reliability and design quality in software used in safety systems.[1] In particular, the methods are consistent with GDC 1 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 the maintenance and control of appropriate records of software development activities. 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 software elements if those systems include software.

Purpose of Regulatory Guides

The NRC issues RGs to describe methods the NRC 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 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 during staff review of 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, respectfully. 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

Description of Change

This revision to RG 1.169 addresses two new areas within IEEE Std. 828-2005. The first is addressed by the addition of a new Staff Regulatory Guidance position 12, "Release Management and Delivery." IEEE Std. 828-2005 has added this new section in order to control the overall software release management objectives. This new area for the "software configuration management" (SCM) complements the existing standard work found in the software life-cycle project plan.

The second new area refers to security features or mechanisms which can play a critical role in supporting software security at higher levels of assurance. IEEE Std. 1012-2004, "IEEE Standard for Software Verification and Validation," (Ref. 7), as endorsed by RG 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Ref. 8) requires a security analysis be performed during the development, operation, and maintenance life cycle processes. IEEE Std. 828-2005 adds to this by requiring measures to control security information such as the results of security analyses. To meet criteria of IEEE Std. 603-1991 and 10 CFR 50, Appendix B, the controlled development of digital safety system software is to be performed in a secure development and operational environment (SDOE). For guidance to establish an SDOE, refer to RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," (Ref. 9).

This RG is based on standards and describes methods acceptable for any safety system software and discusses the required SCM activities. It is the responsibility of the applicant or licensee to determine how the required activities will be implemented.

Background

The use of industry 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. Compliance with these standards does not guarantee that regulatory requirements will be met. However, such 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 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." The identification, control, and documentation of safety system software must be accomplished as part of the effort to comply with NRC requirements. In addition to the record maintenance requirement of GDC 1, Appendix B provides detailed quality assurance criteria, including criteria for administrative control, design documentation control, design interface control, design change control, document control, identification and control of parts and components, and control and retrieval of qualification information associated with parts and components. For software, these activities are often referred to collectively as SCM.

Several criteria in Appendix B of 10 CFR Part 50 contain requirements closely related to configuration management activities. These listed criteria are only part of and not the entire requirement:

- Criterion II, "Quality Assurance Program," requires, in part, that activities affecting quality be accomplished under suitably controlled conditions.

- Criterion III, “Design Control,” requires, in part, that measures be established for design documentation and the identification and control of design interfaces. This criterion also requires that design changes be subject to design control measures commensurate with those used for the original design.

- Criterion V, “Instructions, Procedures, and Drawings,” requires, in part, activities affecting quality be prescribed by documented instructions, procedures, or drawings of a type appropriate to the circumstances and that these activities be accomplished in accordance with these instructions, procedures, or drawings. Criterion V further requires that instructions, procedures, and drawings include appropriate quantitative or qualitative acceptance criteria for determining that important activities have been satisfactorily accomplished.

- 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 be established to ensure that purchased material conforms to the specifications in procurement documents.

- Criterion VIII, “Identification and Control of Materials, Parts, and Components,” requires, in part, that parts and components be identified to prevent the use of incorrect or defective parts or components.

- Criterion XIII, “Handling, Storage and Shipping,” requires, in part, that measures be established to control handling, storage, shipping, and preservation of materials to prevent damage.

- Criterion XIV, “Inspection, Test, and Operating Status,” requires, in part, that measures be established to indicate the status of inspections and tests and the identification of items passing the inspections and tests.

- Criterion XVI, “Corrective Action,” requires, in part, that conditions adverse to quality, such as failures, malfunctions, and deficiencies, be identified and that the cause be determined, the condition be corrected, and the entire process be documented.

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

- Criterion XVIII, “Audits,” requires, in part, that a comprehensive system of audits be conducted, results of those audits be documented, and follow-up actions taken where indicated.

Configuration management is a significant part of engineering activities and is already addressed by NRC requirements for structures, systems, and components important to safety. Although the principles and intentions of traditional configuration management apply equally to software, software involves a significant change in emphasis for which traditional hardware configuration management systems might not be sufficient. Software requires a greater emphasis on the design process, and the deliverable product is more like a design output. In the production of engineered hardware, design outputs are typically inputs to a manufacturing or construction process, and configuration management activities focus on ensuring that design outputs and manufacturing or construction process variables are traceable to identifiable manufactured or construction products. In contrast, in the production of engineered software, design process information may result in the development of many intermediate design outputs generally associated with the final design output. Typically, numerous software engineering changes are expected and encountered during the coding and testing phases. Consequently, although similar in intent to hardware configuration management, SCM requires a change in emphasis and the expansion of the importance of intermediate design baselines and associated design process information. Appropriate SCM records accurately capture every change and provide a reliable and powerful tool to compare every difference between any two intermediate versions of a software implementation. The need for robust and detailed change management and for rigorous identification and control of product versions is also substantially increased.

One consensus standard on software engineering, IEEE Std. 828-2005, as endorsed by this RG, describes software industry approaches to SCM that are generally accepted in the software engineering community. This standard provides guidance for planning and executing a SCM program. Software configuration management is a formal engineering discipline that is a part of an overall system configuration management process. Software configuration management provides the methods and tools used to identify and control software throughout its development and use. The IEEE Std. 828-2005 elaborates on the important features required in an SCM program that traditional hardware configuration management programs may underemphasize. The software engineering community recognizes that the development of an effective SCM program hinges upon a well-defined software configuration management plan.

Clause 3.3 of IEEE Std. 828-2005 describes seven functional areas for grouping configuration management activities:

1. configuration identification (Clause 3.3.1),
2. configuration control (Clause 3.3.2),
3. configuration status accounting (Clause 3.3.3),
4. configuration evaluation and reviews (Clause 3.3.4),
5. interface control (Clause 3.3.5),
6. subcontractor/vendor control (Clause 3.3.6), and
7. release management and delivery (Clause 3.3.7).

However, while IEEE Std. 828-2005 requires that SCM plans describe provisions for these activities, the standard has no minimum set of activities for safety system software. Staff Regulatory Guidance position 4 of this RG specifies a minimum set of the safety system software activities.

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. 10) discusses the importance of configuration management plans for computer software used in safety related systems. This RG incorporates similar configuration management 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

This RG applies to all aspects of the software life cycle within the system life-cycle context. IEEE Std. 828-2005 provides an approach that the NRC staff considers acceptable for satisfying the agency's regulatory requirements with respect to configuration management plans for safety system software with the exceptions and additions listed in these regulatory positions. In this section of the guide, the cited criteria refer to Appendix B to 10 CFR Part 50 unless otherwise noted.

1. Definitions

IEEE Std. 828-2005 refers to IEEE/Electronic Industries Association (EIA) 12207.0-1996, "Industry Implementation of International Standard ISO/IEC 12207:1995 (ISO/IEC 12207) Standard for Information Technology-Software Life Cycle Processes," issued March 1998 (Ref. 11), for definitions of the technical terms that are enumerated in Clause 2 of IEEE Std. 828-2005. These definitions are acceptable with the clarifications and additions noted below.

a. Baseline. Meaning (1) of the term "baseline" from IEEE Std. 828-2005 is to be used. "Formal review and agreement" is considered to mean that responsible management has reviewed and approved a baseline. Baselines are subject to change control. Regulatory Position 2 of this regulatory guide describes the acceptable baseline change approval authority.

b. Interface. All four variations of the meaning of the term "interface" in IEEE Std. 828-2005 are to be used, depending on the context. Meaning (1), "a shared boundary across which information is passed," is interpreted broadly according to Criterion III to include design interfaces between participating design organizations.

c. Configuration Audit. In the context of an audit for delivery of a product, a configuration audit includes both a functional configuration audit and a physical configuration audit.

2. Authority Levels

Hierarchies of change approval authority levels are permitted, provided that the required authority level is commensurate with the life-cycle stage (nearness to release) and the product's importance to safety. The promotion of a software product from one level of safety significance to another level of safety significance could involve a change in level of control (as described in Clause 3.3.2.3 of IEEE Std. 828-2005) and a change in responsible individual.

3. Acceptance Criteria

The SCM plan should describe the criteria for selecting control points, as defined in Clause 2.1.1 of IEEE Std. 828-2005, and establish the correspondence between control points identified in the plan and baselines, project milestones, and life-cycle milestones.

4. Configuration Management

The minimal set of safety system software activities to be covered by the SCM plan should accomplish the following:

a. identification and control of all software designs and code;
b. identification and control of all software design interfaces;
c. control of all software design changes;
d. control of software documentation (user, operating, and maintenance documentation);
e. control of software vendors supplying safety system software;
f. control and retrieval of qualification information associated with software designs and code;
g. software configuration audits;
h. status accounting; and
i. control of building, release, and delivery of products.

Other quality assurance activities may serve or control some of these functions; in that case, the SCM plan should describe the division of responsibility.

An SCM program that complies with IEEE Std. 828-2005 should take control of contractually developed or qualified commercial software products that are safety system software. This means, for example, that the exact version of the product should be identified and controlled according to the change control procedures applied to other configuration items, and the SCM system should track and report its usage.

5. Corrective Action

Criterion XVI requires, in part, that conditions adverse to quality, such as failures, malfunctions, and deficiencies, are identified and that the cause be determined, the condition be corrected, and the entire process be documented. In software development or maintenance activities, the responsibility for these activities is often distributed among several organizations, possibly leading to a fragmented view of the correction process. Clause 3.3.2 of IEEE Std. 828-2005 requires a description of the correction process, including change requests, change evaluation, change approval, change implementation, change verification, and changed-version release. The preliminary steps leading to a change request should also be described, including the responsibility for executing and documenting anomaly reports, problem analyses, and statistical monitoring of software performance. If other documents describe these activities, the descriptions may be included by reference to those documents.

6. Documentation

Clause 3.3.1.1 of IEEE Std. 828-2005 requires, as a minimum, that the SCM plan lists all configuration items to be delivered. This meets the requirements of Criterion VIII with regard to safety system software if all software deliverables are identified and controlled as configuration items. It also meets the requirements of Criteria III, VI, and VII.

For safety system software, configuration items or controlled documents should include the following:

a. software requirements, designs, and code;
b. data files used and called directly or indirectly by software;
c. support software used in development (exact versions);
d. libraries of software components essential to safety;
e. software plans that could affect quality;
f. test software requirements, designs, or code used in testing;
g. test results used to qualify software;
h. analyses and results used to qualify software;
i. software documentation;
j test cases;
k. databases and software configuration data; and
l. software change documentation.

Items that could change because of design changes, review, or audit should be configuration items subject to formal change control. Other items, such as compilers, that may not change but are necessary to ensure correct software production should also be configuration items, thereby ensuring that all factors contributing to the executable software are controlled. This also is useful in areas such as maintenance, future software development, and tracing the impact of reported errors, faults, and the performance of appropriate regression analysis to support the acceptance of future changes to the software. Items that are retained for historical or statistical purposes may be controlled documents.

7. Control of Purchased Materials

The SCM program that complies with IEEE Std. 828-2005, as endorsed by this RG, should take control of contractually developed or qualified commercial software products that are safety system software. This meets the requirements of Criteria VII and VIII with regard to safety system software. This means, for example, that the exact version and build number of the product should be identified and controlled according to the change control procedures applied to other configuration items, and the product's usage should be tracked and reported.

For the use of commercial grade software in safety related digital systems, additional detailed information on acceptance processes appears in Electric Power Research Institute (EPRI) Topical Report (TR)-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," issued October 1996 (Ref. 12), which was endorsed by an NRC safety evaluation report (SER) dated July 17, 1997 (Ref. 13).

8. Development Tools

Tools used in the development of safety system software should be handled according to IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power

Generating Stations," issued 2003 (Ref. 14), as endorsed by RG 1.152. In particular, an SCM program operated by the using organization that complies with IEEE Std. 828-2005 should take control of tools (i.e., tools should be treated as configuration items). SCM Plans should identify that software tools used in the production of safety system software be considered as a configuration item.

9. Acceptance Criteria

Clause 4.2, "Downward Adaptation," of IEEE Std. 828-2005 specifies conditions under which some requirements in the standard may be omitted when deemed not applicable to a particular scope, limited complexity, or unusual environment for a project. In order to maintain acceptance criteria established in accordance with Criterion V and suitably controlled conditions (in accordance with Criteria II and VIII) for safety system software, this regulatory guide does not endorse this clause.

10. Design Verification

Clause 3.3.2(d) of IEEE Std. 828-2005 requires a definition of the verification, implementation, and release of a change. The criteria for verification must meet the requirements of Criterion III, which requires that design changes be subject to design control measures commensurate with those applied to the original design. This encompasses the reexamination of any appropriate safety analysis related to the change.

11. Software Configuration Management Plan

Clause 3.1(g) of IEEE Std. 828-2005 requires the SCM plan to address the assumptions upon which the plan is based, including assumptions that might have an impact on cost and schedule. Any use of cost and schedule criteria must be consistent with the requirement of 10 CFR 50.57(a)(3) that there be reasonable assurance that the activities authorized by the operating license can be conducted without endangering public health and safety.

12. Release Management and Delivery

Clause 3.3.7 of IEEE Std. 828-2005 requires that the SCM plan describe how the building, release, delivery, change control, master copies of code, and documentation of software will be formally controlled "in accordance with the policies of the organizations involved." This control should include the preservation of materials used to deliver the software and a change control mechanism sufficient to ensure the correction of faults identified in the software.

13. Backfit Clarification

Clause 1.1 of IEEE Std. 828-2005 states: "It also applies to noncritical software and to software already developed." Such statements in the standard should not be interpreted as requirements for backfit as defined in 10 CFR 50.109, "Backfitting." Section D of this RG provides the NRC staff position on backfitting as it concerns this guidance.

14. Annexes

IEEE Std. 828-2005 contains two informative annexes. These annexes are listed here as sources of information; they have not received regulatory endorsement unless otherwise noted:

Annex A, "Bibliography," lists IEEE standards that are useful in implementing and interpreting the test requirements contained in IEEE Std. 828-2005. The paragraph titled "Other Codes and

Standards" in Section B of this regulatory guide provides the NRC staff position on the endorsement and use of other standards.

Annex B, "Relationship of IEEE Std. 828-2005 to Other Standards," describes the relationship of IEEE Std. 828-2005 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, and International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) Technical Report (TR)-19759:2005, "Software Engineering-Guide to the Software Engineering Body of Knowledge (SWEBOK)," issued 2005 (Ref. 15). The NRC does not endorse this annex because the agency has endorsed neither IEEE/EIA Std. 12207.1-1997 nor ISO/IEC TR-19759:2005.

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.

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. 16) and the NRC Management Directive 8.4, "Management of Facility-Specific Backfitting and Information Collection" (Ref. 17).

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

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.

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

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

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

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

10. 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.[6]

11. Institute of Electrical and Electronics Engineers and Electronic Industries Association (IEEE/EIA) Std. 12207.0-1996, “Industry Implementation of International Standard ISO/IEC 12207:1995 (ISO/IEC 12207) Standard for Information Technology - Software Life Cycle Processes,” IEEE/EIA, Engineering Department, Piscataway, NJ, March 1998.

[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.

[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

12. Electric Power Research Institute (EPRI) TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," Palo Alto, CA, 1996.[7]

13. Letter from Matthews, D. B., Chief, Generic Issues and Environmental Projects Branch, Division of Reactor Program Management, NRC, to Torok, R.C., Project Manager, Nuclear Power Group, EPRI, dated July 17, 1997, titled "Review of EPRI topical report TR-106439, 'Guideline on Evaluation and Acceptance of commercial Grade digital Equipment for Nuclear Safety Applications' (TAC No. M94127)" (ADAMS Accession No. ML092190664).

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

15. International Organization for Standardization (ISO) Std. ISO/IEC TR 19759:2005, "Software Engineering - Guide to the Software Engineering Body of Knowledge (SWEBOK)," Geneva, Switzerland, 2005.[8]

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

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

[7] Copies of the listed Electric Power Research Institute (EPRI) standards and reports may be purchased from EPRI, 3420 Hillview Ave., Palo Alto, CA 94304; telephone 800-313-3774; fax 925-609-1310.

[8] 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 online at the ISO Store Web site: http://www.iso.org/iso/store.htm.