U.S. NUCLEAR REGULATORY COMMISSION

July 2013
Revision 2

Technical Lead
Karl Sturzebecher

# REGULATORY GUIDE

OFFICE OF NUCLEAR REGULATORY RESEARCH

## REGULATORY GUIDE 1.168

*(Draft was issued as DG-1267, dated August 2012)*

# VERIFICATION, VALIDATION, REVIEWS, AND AUDITS FOR DIGITAL COMPUTER SOFTWARE USED IN SAFETY SYSTEMS OF NUCLEAR POWER PLANTS

## A. INTRODUCTION

### Purpose

This regulatory guide (RG) describes a method the staff of the U.S. Nuclear Regulatory Commission (NRC) considers acceptable for use in complying with NRC regulations with respect to verification, validation, reviews, and audits for digital computer software used in 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 verification, validation, reviews, and audits 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, "Quality Standards and Records," requires, in part, that quality standards be established and implemented to provide adequate assurance that structures, systems, and components important to safety will satisfactorily perform their safety functions. Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," to 10 CFR Part 50, describes criteria that must be met by a quality assurance program for structures, systems, and components (SSCs) that prevent or mitigate the consequences of postulated accidents. In particular, besides the SSCs that directly prevent or mitigate the consequences of postulated accidents, the criteria of Appendix B also apply to all activities, such as designing, purchasing, installing, testing, operating, maintaining, or modifying, that affect the safety-related functions of such SSCs.

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. 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, "IEEE Standard 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

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. ML13073A2103. The regulatory analysis may be found in ADAMS under Accession No. ML103160461 and the staff responses to the public comments on DG-1267 may be found in ADAMS under Accession No. ML12354A517.

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. This guidance on the safety systems equipment employing digital computer software or firmware requires quality standards for verifying and validating computer software used in safety systems of nuclear power plants.

This RG endorses IEEE Std. 1012-2004, "IEEE Standard for Software Verification and Validation" (Ref. 4), and IEEE Std. 1028-2008, "IEEE Standard for Software Reviews and Audits" (Ref. 5). IEEE Std. 1012-2004, with the exceptions stated in the staff regulatory guidance of this RG, describes a method acceptable to the NRC staff for complying with NRC regulations for promoting high functional reliability and design quality in software used in safety systems.[1] In particular, the method is consistent with GDC 1 in Appendix A to 10 CFR Part 50 and the criteria for quality assurance programs in Appendix B, as they apply to software verification and validation (V&V). The criteria of Appendices A and B of 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. IEEE Std. 1028-2008 provides guidance acceptable to the NRC staff for carrying out software reviews, inspections, walkthroughs, and audits subject to certain provisions.

**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 NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," Chapter 7, "Instrumentation and Controls," (the Standard Review Plan) (Ref. 6). The NRC staff uses the NRC Standard Review Plan when reviewing 10 CFR Part 50 and 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants," (Ref. 7) 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

**Reason for Revision**

The original version of this RG endorsed IEEE Std. 1012-1998 and IEEE Std. 1028-1997. This revision endorses the updated versions of both IEEE standards. One of the main differences between the 2008 and 1997 versions of IEEE Std. 1028 is the addition of an anomaly ranking and reporting found in Clause 6.8.3. This system for reporting anomalies should be considered beneficial and useful to the applicants and licensee when addressing the anomaly reporting documentation requirements found in IEEE Std. 829-2008, "IEEE Standard for Software and System Test Documentation," (Ref. 8).

**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 consensus standards does not guarantee that regulatory requirements will be met. However, compliance with consensus standards 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 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 (I&C) systems covered by Appendix B to 10 CFR Part 50 as "safety system software." For safety system software, software V&V, reviews, and audits are important parts of the effort to comply with NRC requirements. Software engineering practices rely, in part, on software V&V and on technical reviews and audits to meet general quality and reliability requirements in General Design Criteria 1 and 21, "Protection System Reliability and Testability," of Appendix A to 10 CFR Part 50, as well as Criteria II, III, XI, and XVIII of Appendix B. In addition, management reviews and audits of software processes are part of a verification process consistent with Criterion I of Appendix B.

Several criteria in Appendix B to 10 CFR Part 50 requiring the development of a quality assurance program would also be relevant to the development of an effective software V&V, review and audit process. These requirements include:

- Criterion I, "Organization," specifies that applicants must (1) assure that an appropriate quality assurance program is established and effectively executed, and (2) verify (for example, by checking, auditing, and inspection) that activities affecting safety-related functions have been correctly performed.

- Criterion II, "Quality Assurance Program," requires, in part, that activities affecting quality be accomplished under suitably controlled conditions. Controlled conditions include the use of appropriate equipment, suitable environmental conditions for accomplishing the activity, and assurance that all prerequisites for the given activity have been satisfied. The criterion also requires that the program considers the need for verification of quality by inspection and test.

- Criterion III, "Design Control," requires, in part, that design control measures provide for verifying or checking the adequacy of design.

- Criterion XI, “Test Control,” requires, in part, that a test program be established to assure that all testing required to demonstrate that structures, systems, and components will perform satisfactorily in service is identified and performed in accordance with written test procedures which incorporate the requirements and acceptance limits contained in applicable design documents.

- Criterion XVII, “Quality Assurance Records,” requires, in part, retention of records to furnish evidence of activities affecting quality. The records shall include identification and descriptions of actions taken in connection with any changes or design deficiencies noted.

- Criterion XVIII, “Audits,” requires, in part, that a comprehensive system of planned and periodic audits be carried out to verify compliance with all aspects of the quality assurance program and to determine the effectiveness of the program.

**Description of Change**

Technical reviews, some audits, and software inspections and walkthroughs focus on the V&V of products of the software development process. Management reviews and other audits are focused on ensuring that planned activities are being accomplished effectively. Reviews and audits are closely associated with V&V activities since technical reviews and audits are frequently conducted by the V&V organization and because the V&V organization normally participates in management reviews. Because of this close connection of the V&V activity with reviews and audits, this RG addresses IEEE Std. 1012-2004 and IEEE Std. 1028-2008 together.

The IEEE Std. 1012-2004 revision has several changes from the in 1998 version. The first of which is the addition of a conditional independence option in Annex C, Table C.1, and the second is the addition of a new activity called “Security Analysis.” Another noticeable change with the 2004 revision is the recommended use of the software integrity system, as the previous version did not require the selection of an integrity level. This RG addresses these integrity levels in Section C, “Staff Regulatory Positions,” position 1, titled “Software Integrity.”

In response to the first change, RG 1.168, Staff Regulatory Guidance position 3 has an additional perspective on the topic of independence and provides clarification for organizational mapping as per IEEE Std. 1012-2004, Annex F. The new IEEE concept of conditional independence in Annex C, Table C.1 is not acceptable to the NRC staff. The NRC staff finds the second change in IEEE Std. 1012-2004 called “Security Analysis,” to be consistent with a life-cycle approach and has altered the RG 1.168 position in Part C, 7.c, to what is now called a “Secure Analysis.” This RG has expanded the equipment that must be protected by physical barriers and access control from that identified in the 2004 version of the RG.

IEEE Std. 1012-2004 established a new task for many of the V&V activities called "Security Analysis" (see Table 1 for a comprehensive overview of the application of this new task). This new security analysis task is intended to address accidental and malicious activities that can affect the software. The NRC does not support this activity as a means to address malicious acts that may damage the software. Furthermore, the NRC has established a V&V life-cycle approach for the accidental or non-malicious acts by providing a secure development and operational environment (SDOE) guidance when developing a digital safety system. To meet criteria of IEEE Std. 603-1991 and 10 CFR 50, the development of digital safety system software requires an SDOE. RG 1.152 provides specific guidance concerning the establishment of SDOEs. The NRC staff recognizes that SDOE features or mechanisms can also play a critical role in supporting software security at higher levels of assurance.

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. Specifically a licensee's adherence to the provisions of 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks," (Ref. 9) will be evaluated per regulatory programs specific to that regulation and in accordance with the applicant's NRC-approved cyber security plan. IEEE Std. 1012-2004 and 1028-2008 are not endorsed in this RG as being appropriate for compliance with 10 CFR 73.54.

**Related Guidance**

Industry standard IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations" (Ref. 10), which is endorsed by RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants" (Ref. 11), and Committee on Nuclear Quality Assurance of American Society of Mechanical Engineers (ASME/NQA) standard ASME/NQA-1-2008, "Quality Assurance Requirements for Nuclear Facility Applications" (Ref. 12), describe general design verification processes, but do not detail software V&V planning and the conduct of reviews and audits. Two consensus standards on software engineering, IEEE Std. 1012-2004 and IEEE Std. 1028-2008, describe the software industry's approaches to software V&V, review, and audit activities that are generally accepted in the software engineering community. Meeting these standards helps to meet regulatory requirements by ensuring that disciplined software V&V, review, and audit practices accepted within the software community will be incorporated into software processes applied to safety system software. IEEE Std. 1012-2004 describes the process of software V&V, including elements of a software V&V plan (SVVP), and describes a minimum set of V&V activities for software at different integrity levels. IEEE Std. 1028-2008 is a process standard that provides guidance for conducting technical and management reviews, inspections, walkthroughs, and audits.

With consideration of the different standards used in software development the applicant or licensee should consider the hierarchy of the different standards for guidance. IEEE Std. 1074-2006, "IEEE Standard for Developing Software Life Cycle Processes" (Ref. 13), as noted in RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software in Safety Systems of Nuclear Power Plants" (Ref. 14), should be reviewed as the main outline standard when working with this RG.

This RG is based on standards the NRC staff considers acceptable for any safety system software and it discusses the required V&V activities. It is the responsibility of the applicant or licensee to determine the specifics of 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. 15), discusses the importance of validating computer codes used in safety related systems. This RG incorporates similar verification and validation recommendations and is consistent with the basic safety 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 an 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. 1012-2004 provides an acceptable approach to the NRC for meeting the agency's regulatory requirements on the V&V of safety system software with the exceptions and additions listed in this staff regulatory guidance section. In this section of the guide, the cited criteria refer to Appendix B to 10 CFR Part 50 unless otherwise noted.

The methods in IEEE Std. 1028-2008 provide an approach acceptable to the NRC staff for carrying out software reviews, inspections, walkthroughs, and audits, subject to the exceptions and additions listed in these regulatory positions. These methods are often used in association with software quality assurance activities.

The annexes to IEEE Std. 1012-2004 and IEEE Std. 1028-2008 contain information that may be useful. However, the information in these annexes should not be viewed as the only possible solution or method. Since the nuclear industry has not reached a consensus regarding the use of these methods, the NRC staff does not endorse the use of these annexes, except as noted below.

## 1. Software Integrity

Clause 4 of IEEE Std. 1012-2004 defines an acceptable four-level method of quantifying software integrity levels, in which level 4 is the highest and level 1 the lowest. The standard uses software integrity levels to determine the minimum V&V tasks to be performed. The applicant or licensee may either use the method in the standard or define another method and provide mapping between the applicant's or licensee's method and the method defined in the standard. Software used in nuclear power plant safety systems should be assigned integrity level 4 or the equivalent, as demonstrated by a mapping between the applicant or licensee approach and integrity level 4 as defined in IEEE Std. 1012-2004.

The NRC staff takes exception to the Table B.1, "Assignment of software integrity levels" and Table B.3 "Graphic illustration of the assignment of the software integrity levels" in Annex B. In Table B.1 the system description "critical consequences" is not acceptable as a task description for level 4. The IEEE Std. 1012-2004 statement about the Table B.3 illustration for determining the likelihood and evaluating software integrity level lower than Level 4 is not acceptable. Additionally the NRC staff interprets the phrase "no mitigation possible" within Clause 4, Software integrity levels, as a mitigation

reference within the given safety system's safety function only. To maintain the overall plant level safety function, a diverse system may be used to provide reasonable assurance of completion. The licensee or applicant should assign integrity level 4 or the equivalent to software used in nuclear power plant safety systems, as demonstrated by a mapping between its approach and integrity level 4.

**2. Software Reliability**

Criteria III requires verifying or checking the adequacy of design and Table 1 of IEEE Std. 1012-2004 provides an acceptable approach for software reliability verification or testing. The component and integration test plans in Table 1 describe methods for measuring software reliability that should serve as criterion for determining if software elements correctly implement software requirements (see 5.4.3, "Activity: Design V&V," Task 5, "Component V&V test plan generation," and Task 6, "Integration V&V test plan generation").

In addition, to complement and remain consistent with the staff's position on reliability measures for digital safety systems contained in other agency guidance, the NRC staff's acceptance of quantitative reliability goals for computer-based safety systems is predicated on deterministic criteria for the computer system in its entirety (i.e., hardware, system software, firmware, application, and interconnections).

**3. Independence of Software Verification and Validation**

Criterion I requires that persons and organizations performing quality assurance functions report to a management level such that sufficient authority and organizational freedom exist, including sufficient independence from cost and schedule limitations. Quality assurance functions include verifying, such as by checking, auditing, and inspecting, that activities affecting the safety related functions have been correctly performed. Criterion III imposes an independence requirement for the verification and checking of the adequacy of the design, requiring that those who perform the verification and checking be persons other than the designers.

Accordingly, any organization with reviewers performing the verification function should not be part of the design organization's development effort, and should use an independent organizational structure with regard to technical, financial and managerial independence of its reviewers that is not subject to the budgetary and scheduling constraints of the design organization or project management function. In pursuit of this concept, the mapping of an organizational model should demonstrate how the staff reviewers are independent and exclusive to the tasking areas. The Figure F.1 in Annex F of IEEE Std. 1012-2004 is acceptable to the NRC, however this only applies to the tasking areas in the top three relationship boxes: "Acquire Program Management," "V&V Effort," and "Development Effort." As per this regulatory guidance, the bottom three "Staff" boxes and relationship lines are excluded.

The applicant or licensee has ultimate responsibility for the adequacy of V&V and the quality of subsequent safety system software. This is particularly important when an external organization has performed the V&V tasks (e.g., a licensee acquires a commercial-grade product approved by the NRC staff for implementation in a safety-related system). In these cases, the applicant or licensee is not relieved of the responsibility for ensuring that the V&V and subsequent software quality satisfy NRC requirements for reliability. Thus, the applicant or licensee should verify that the extent of independence between the organization responsible for design and the organization responsible for verification and checking of the design meets NRC requirements in Appendix B. This level of financial, managerial and technical independence is to be sufficient to ensure that schedule and resource demands placed on the design process do not compromise the V&V process. Criterion II states that the program must provide for indoctrination and training of personnel performing activities affecting quality as necessary to ensure that suitable proficiency is achieved and maintained. The independent verifiers should be at least as

proficient, and preferably more proficient in both software engineering and I&C safety system functionality and design to ensure that software V&V is adequately implemented.

IEEE Std. 1012-2004 provides guidance for establishing financial, managerial, and technical independence for software V&V. Criterion I of Appendix B requires that persons and organizations performing quality assurance functions report to a management level such that they have authority and organizational freedom, including independence from cost and schedule considerations, sufficient to identify quality problems; initiate, recommend, or provide solutions; and verify implementation of solutions. Specifically, there shall be an acceptable organizational structure, including mapping of that structure, to what constitutes a sufficient application of an independent verification and validation (IV&V) organization. The guidance in IEEE Std. 1012-2004 for financial independence provides appropriate freedom with respect to the V&V organization's budget, and the standard's guidance for managerial independence provides appropriate freedom with respect to V&V schedules, as well as overall project cost and schedule considerations.

Similarly, the IEEE Std. 1012-2004 guidance for technical independence satisfies the requirements in Criterion III of Appendix B that design verification or checking be performed by individuals or groups other than those who prepared the original design. Note that Clause C.4.1 of IEEE Std. 1012-2004 states that the V&V responsibility "is vested in an organization that is separate from the development organization." The NRC staff position is that this does not mean that a separate company should perform independent V&V. However, the requirements specified in Criteria I and III of Appendix B described above must be met.

## 4. Conformance of Materials

Criterion III states that measures are to be established for the selection and review for suitability of application of materials, parts, equipment, and processes that are essential to the safety-related functions of the structures, systems, and components to which Appendix B applies. Criterion VII states that measures are to be established to ensure that purchased material, whether purchased directly or through contractors and subcontractors, conforms to the procurement documents. IEEE Std. 1012-2004 provides guidance for retrospective V&V of software that was not verified. Specifically, Clauses 1.1, 1.5, 4, 5.4.4, Task 1 of Activity 5.6.1 in Table 1, and Annex D discuss V&V of preexisting (pre-developed) software (e.g., commercial off-the-shelf). This RG does not endorse the use of this guidance for the acceptance of preexisting (pre-developed) safety system software. 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) Topical Report (TR)-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," issued October 1996 (Ref. 16), which was accepted by an NRC issued safety evaluation report (SER) dated July 17, 1997 (Ref. 17).

## 5. Quality Assurance

Criterion I identifies the quality assurance functions of (1) assuring that an appropriate quality assurance program is established and effectively executed and (2) verifying, such as by checking, auditing, and inspecting, that activities affecting the safety-related functions have been correctly performed. Criterion III requires that design changes be subject to design control measures commensurate with those applied to the original design. In addition to the provisions of IEEE Std. 1012-2004 (in Clause 7.7.4) regarding control procedures, any V&V materials necessary for the verification of the effectiveness of the V&V programs or necessary to furnish evidence of activities affecting quality should be maintained as quality assurance records. The records necessary for the

verification of changes should be maintained in accordance with Criterion XVII, which also requires that sufficient records be maintained to furnish evidence of activities affecting quality.

## 6. Tools for Software Development

Tools used in the development of safety system software should be handled according to IEEE Std. 7-4.3.2-2003, as endorsed by RG 1.152. However the V&V tasks of witnessing, reviewing, and testing are not required for software tools, provided the software that is produced using the tools is subject to V&V activities that will detect flaws introduced by the tools. If this cannot be demonstrated, the provisions of this RG are applicable to the development of tools.

## 7. Verification and Validation Tasks

Table 3 of IEEE Std. 1012-2004 lists "optional" V&V tasks. Annex G (which is for information only) to IEEE Std. 1012-2004 further describes these tasks. They are intended to provide a tailoring capability by allowing tasks to be added to the minimum set for safety-related software. The NRC staff takes exception to the "optional" status of some tasks on this list; the staff considers them to be necessary components of acceptable methods for meeting the requirements of Appendices A and B to 10 CFR Part 50 as applied to safety system software, regardless of whether they are performed by the V&V organization. The NRC staff considers the following tasks to be part of the minimum set of V&V activities for safety-related software unless they are (1) incorporated into other V&V tasks in the SVVP or (2) performed outside the software V&V organization as part or all of the duties of some other organization:

a. Audits

Criterion I of Appendix B defines quality assurance functions as including verification, such as by checking, auditing, and inspecting, that activities affecting safety-related function have been correctly performed. Criterion III requires design control measures for verifying or checking the adequacy of design. Safety system software V&V organizations should employ audits, including functional audits, in-process audits, and physical audits of software. Although these audits are commonly considered to be the responsibility of the software quality assurance organization and the configuration management organization, they should be performed and relied on by the V&V organization. If so, the audits should be described in the SVVP. IEEE Std. 1028-2008 describes an acceptable method of conducting these audits.

b. Regression Analysis and Testing

Criterion III requires that design changes be subject to design control measures commensurate with those applied to the original design. Regression analysis and testing following the implementation of software modifications is an element of the V&V of software changes and should be part of the minimum set of software V&V activities for safety system software.

c. Secure Analysis

IEEE Std. 1012-2004 lists "security analysis" as a V&V task and part of the life-cycle V&V activities. Clause 7.7.4 provides guidance on control procedures applied to the V&V effort to protect software products and V&V results from unauthorized alterations. These V&V tasks should be designed to test the secure operational environment design features of the safety system software. The security related V&V tasks should not only verify and validate the SDOE feature

criteria and functions, but also assure protection from inadvertent manipulation of the test environment and test results.

The security analysis V&V tasks activities may be addressed in a separate document or as part of one or more of the other documents. Measures taken to secure the test environment and processes should address the V&V test phase vulnerabilities identified in the vulnerability assessment. The NRC staff may review and audit any of the documentation and/or V&V security analysis and testing to conclude that the digital safety system was developed in a secure environment and that it will be protected from inadvertent actions in its operational environment. In addition RG 1.152 contains guidance on the establishment of SDOEs for digital safety systems to meet criteria of IEEE Std. 603-1991 and 10 CFR 50, Appendix B.

d. Test Evaluation

Test evaluation includes confirming the technical adequacy of test materials such as plans, designs, and results. These materials should be evaluated for consistency with Criterion II, in its requirement for controlled conditions, and with Criterion XI, in its requirement for the evaluation of test results.

e. Evaluation of User Documentation

User documentation is important to the safe operation and proper maintenance of safety system software. The requirements of Criterion III for correctly translating the design basis of safety system software into specifications, procedures, drawings, and instructions apply to software documentation, including user documentation.

## 8. Annexes

There are eight informative annexes in IEEE Std. 1012-2004, while IEEE Std. 1028-2008 contains two informative annexes. These annexes are listed here as sources of information; they have not received regulatory endorsement unless otherwise noted:

IEEE Std. 1012-2004:

- Annex A, "Mapping of IEEE Std. 1012 V&V Activities and Tasks," provides the mappings of IEEE Std. 1012-2004 V&V activities to V&V requirements of the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 12207:1995, "Information Technology-Software Life Cycle Processes" (Ref. 18); IEEE Std. 1074-1997, "IEEE Standard for Developing Software Life Cycle Processes"; and Software Engineering Process Groups' capability maturity model integrated (CMMI) process areas. The NRC does not endorse this annex because it provides no guidance for implementing this standard. However applicants and licensees may find it useful, when integrating elements of these standards into their V&V programs.

- Annex B, "A Risk-based Software Integrity Level Scheme," describes the four software integrity levels and associated consequences. This RG endorses this annex, as described and with the exception noted in Staff Regulatory Guidance position 1.

- Annex C, "Definitions of Independent V&V (IV&V)," defines software independent V&V. The NRC does not endorse this annex, because it provides inadequate guidance.

In Table C.1 the new form of independence provides a conditional option which is not acceptable to the NRC. Branch Technical Position 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems" (Ref. 19) provides additional guidance in this area.

- Annex D, "V&V of Reuse Software," provides options and suggestions to assist the V&V effort of reuse software. The NRC does not endorse this annex because it provides inadequate guidance. Appendix 7.0-A, "Review Process for Digital Instrumentation and Control Systems," and Branch Technical Position 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems" provide additional guidance in this area.

- Annex E, "V&V Measures," describes the measures for evaluating the quality, effectiveness, and efficiency of the V&V tasks. The NRC does not endorse this annex because no consensus exists on measures for evaluating the quality and coverage of the V&V tasks. However, applicants and licensees may find it useful to provide feedback for the continuous improvement of the V&V process and to evaluate the software development processes and products.

- Annex F, "Example of V&V Organizational Relationship to Other Project Responsibilities," provides an organizational structured diagram, Figure F.1, which is endorsed by this RG with one exception. As described in Staff Regulatory Guidance position 3, the top three main organizational boxes; "Acquirer Program Management", "Development Effort," and "V&V Effort" demonstrate an acceptable relationship model; however the bottom three "Staff" boxes with reporting flows are excluded.

- Annex G, "Optional V&V Tasks," describes optional V&V tasks as an effort to provide a tailoring capability by allowing tasks to be added to the minimum set for safety-related software. As described in Staff Regulatory Guidance position 7, the NRC staff considers some of these tasks to be necessary for meeting the regulatory requirements; however Annex G is not endorsed by this RG.

- Annex H, "Bibliography," lists IEEE and ISO/IEC standards that are referenced in IEEE Std. 1012-2004. The bibliography provides sufficient detail to enable licensees to obtain further information regarding specific areas of the standard.

IEEE Std. 1028-2008:

- Annex A, "Comparison of Review Types," compares management review, technical review, inspection, walkthrough, and audit as described within the standard. The NRC does not endorse this annex because it provides no guidance for implementing this standard. However applicants and licensees may find it useful in understanding the difference and the similarities of different types of reviews.

- Annex B, "Bibliography," lists IEEE and ISO/IEC standards that are referenced in IEEE Std. 1028-2008. The bibliography provides sufficient detail to enable licensees to obtain further information regarding specific areas of the standard.

# 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.

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

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.

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.[5]

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

4. IEEE, Std. 1012-2004, "IEEE Standard for Software Verification and Validation," Piscataway, NJ, 2004.

5. IEEE, Std. 1028-2008, "IEEE Standard for Software Reviews and Audits," Piscataway, NJ, 2008.

6. 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, March 2007. (http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0800/ch7/)

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

8. IEEE, Std. 829-2008, "IEEE Standard for Software and System Test Documentation," Piscataway, NJ, 2008.

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

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, Regulatory Guide (RG) 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Washington, DC.

12. ASME International (ASME), NQA-1-2008, "Quality Assurance Requirements for Nuclear Facility Applications," New York, NY, 2008.[6]


---

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 for free 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 ASME International standards may be purchased from ASME International, Two Park Avenue, New York, NY 10016-5990; telephone 800-843-2763. Purchase information is available through the ASME Web site store at http://www.asme.org/kb/standards/standards .

13. IEEE, Std. 1074-1997, "IEEE Standard for Developing Software Life Cycle Processes," Piscataway, NJ, 1997.

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. 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.[7]

16. 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.[8]

17. 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).

18. International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) standard ISO/IEC 12207:1995, "Systems and software engineering - Software life cycle processes," Geneva, Switzerland, 1995.[9]

19. NRC, NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," Chapter 7, "Instrumentation and Controls," Branch Technical Position 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems" Washington, DC, (ADAMS Accession No. ML070670183).

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

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

---

7 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

8 Copies of Electric Power Research Institute (EPRI) documents may be obtained by contacting the Electric Power Research Institute, 3420 Hillview Avenue, Palo Alto, CA 94304, Telephone: 650-855-2000 or on-line at http://my.epri.com/portal/server.pt.

9 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.