U.S. NUCLEAR REGULATORY COMMISSION

July 2013
Revision 1

REGULATORY GUIDE

OFFICE OF NUCLEAR REGULATORY RESEARCH

Technical Lead
Karl Sturzebecher

REGULATORY GUIDE 1.170

(Draft was issued as DG-1207, dated August 2012)

TEST DOCUMENTATION FOR DIGITAL COMPUTER SOFTWARE USED IN SAFETY SYSTEMS OF NUCLEAR POWER PLANTS

A. INTRODUCTION

Purpose

This guide 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 software and system test documentation 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 contains a number of regulations and supporting guidelines applicable to software and system test documentation 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 a quality assurance program be established and implemented to provide adequate assurance that systems and components important to safety will satisfactorily perform their safety functions. GDC 21, "Protection System Reliability and Testability," requires, in part, that the protection system be designed for high functional reliability. 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 systems and components that prevent or mitigate the consequences of postulated accidents. In particular, in addition to the systems and components that directly prevent or mitigate the consequences of postulated accidents, Appendix B criteria also apply to all activities, including design, purchasing, installation, testing, operation, maintenance, or modification, that affect the safety-related functions of such systems and components.

In 10 CFR 50.55a(a)(1) the regulations require, in part, that systems and components be designed, fabricated, erected, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed. 10 CFR 50.55a(h) requires that reactor protection and safety systems satisfy the criteria in Institute of Electrical and Electronics Engineers (IEEE) Standard (Std.) 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" (Ref. 2), including a correction sheet dated January 30, 1995, or in IEEE Std. 279, "Criteria for Protection Systems for Nuclear

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. ML13003A216. The regulatory analysis may be found in ADAMS under Accession No. ML103200047 and the staff responses to the public comments on DG-1207 may be found in ADAMS under Accession No. ML13003A209.

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 and that it 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 test documentation.

This regulatory guide endorses IEEE Std. 829-2008, "IEEE Standard for Software and System Test Documentation," (Ref. 4), with the clarifications and exceptions as described in Secion C, "Staff Regulatory Guidance." IEEE Std. 829-2008 describes methods that the NRC considers acceptable for use in complying with NRC regulations for achieving high functional reliability and design quality in the software used in safety systems.[1] In particular, the methods are consistent with the GDC in Appendix A to 10 CFR Part 50 and the criteria for quality assurance programs in Appendix B to 10 CFR Part 50 as they apply to the documentation of software testing activities. The criteria in Appendices A and B of 10 CFR Part 50 apply to systems and related quality assurance processes, and the requirements extend throughout the life cycle of the protection systems, especially when those systems include software. There are further requirements for software testing which can be found in the documentation retention and handling section of 10 CFR Part 21.51, "Maintenance and Inspection of Records" (Ref. 5).

Purpose of Regulatory Guides

The NRC issues regulatory guides 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 regulatory guides are not substitutes for regulations and compliance with them is not required. The information provided by this regulatory guide 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. 6). 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. 7) license applications.

Paperwork Reduction Act

This regulatory guide 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 number 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.

B. DISCUSSION

Background

The use of industry consensus standards, such as IEEE standards, is part of an overall approach to meet 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, 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

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."

based on experience and represent industry consensus on approaches used for the development of such systems.

This regulatory guide refers to software incorporated into the instrumentation and control systems covered by Appendix B to 10 CFR Part 50 as "safety system software." For safety system software, software testing is an important part of the effort to comply with NRC requirements. Software engineering practices rely, in part, on software testing to meet general quality and reliability requirements consistent with GDC 1 and 21 of Appendix A to 10 CFR Part 50, as well as Criteria I, II, III, V, VI, XI, and XVII of Appendix B.

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

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

- Criterion II, "Quality Assurance Program," requires, in part, that the quality assurance program address the need for the verification of quality through inspections and tests.

- Criterion III, "Design Control," requires, in part, that measures be established for verifying or checking the adequacy of the design (e.g., through the performance of a suitable testing program) and that design control measures should be applied to items such as the delineation of acceptance criteria for inspections and tests.

- Criterion V, "Instructions, Procedures, and Drawings," requires, in part, that 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," and XVII, "Quality Assurance Records," provide for (1) the control of the issuance of documents, including changes thereto, that prescribe all activities that affect quality and (2) the maintenance of sufficient records to furnish evidence of activities that affect quality. The latter requires test records to identify the inspector or data recorder, the type of observation made, the results, the acceptability of the results, and the action taken in connection with any noted deficiencies.

- Criterion XI, "Test Control," requires, in part, establishment of a test program 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 that incorporate the requirements and acceptance limits contained in applicable design documents. Test procedures must include provisions for ensuring that all prerequisites for the given test have been met, that adequate test instrumentation is available and used, and that the test is performed under suitable environmental conditions. Criterion XI also requires that test results be documented and evaluated to ensure that test requirements have been satisfied.

- Criterion XVII, "Quality Assurance Records," requires, in part, retention of records to furnish evidence of activities affecting quality. The record retention requirements should

include,in part, that sufficient quality records be maintained so that specific itemized records for test documentation and controlled by the SCM as the software evolves with development and maintenance are identifiable and retrievable. Test records must identify the inspector or data recorder, the type of observation made, the results, the acceptability of the results, and the action taken in connection with any noted deficiencies.

Accepted practice for the development of software for safety-related applications includes the use of a software life-cycle process that incorporates software testing activities (e.g., IEEE Std. 1074-2006, "IEEE Standard for Developing a Software Life Cycle Process" (Ref. 8)). Software testing is a key element in software verification and validation (V&V) activities, as indicated by IEEE Std. 1012-2004, "IEEE Standard for Software Verification and Validation" (Ref. 9), as endorsed by Regulatory Guide 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Ref. 10), and as indicated by IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations" (Ref. 11), as endorsed by Regulatory Guide 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants" (Ref. 12). The consensus standard, IEEE Std. 829-2008, defines software and system test documentation and specifies its form and content. The term "documentation," used in this regulatory guide, is in accordance with the first meaning of the term given in IEEE Std. 610.12-1990, "IEEE Standard Glossary of Software Engineering Terminology" (Ref. 13), which defines documentation as a collection of documents on a given subject. IEEE Std. 829-2008 describes a method for use in documenting software testing that is consistent with the previously cited regulatory requirements as they apply to safety system software.

The documentation identified in IEEE Std. 829-2008 has expanded in the three existing categories: (1) test planning, (2) test specification, and (3) test reporting. These three categories are consistent with the requirements in Appendix B to 10 CFR Part 50, particularly with the requirements in Criterion XI as they apply to software. The test planning category consists of a test plan with key aspects of an integrity scheme level, which include a life-cycle phase and a traceability matrix for software projects. The overview test plan and report add coverage for further control and details in the test process.

The test specification category describes the details of test designs, test cases, and test procedures that contain the detailed procedures and instructions for testing and the feature or test case acceptance criteria that the licensee will use during the testing effort. This category is particularly relevant to Criterion V.

The IEEE Std. 829-2008 test reporting category consists of an interim status report, an anomaly report, more test logs, along with the final test summary reports that allow the licensee to record and summarize test events and that follow the integrity scheme needed within the life-cycle and serve as the basis for evaluating test results. The final summary report summarizes all category information and addresses the requirements in parts of Criteria VI, XI, and XVII as they apply to software. The documentation in the test reporting category contains most of the specific information itemized in Criterion XVII. However, the change process of the software configuration management (SCM) function, as endorsed by Regulatory Guide 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Ref. 14) will typically address anomaly reporting. IEEE Std. 829-2008 also provides for the inclusion of additional material in its defined documentation; therefore, any special testing information associated with unique circumstances may also be included.

Description of Revision

The IEEE Std. 829-1983 version originally provided a linear test planning, specifications and reporting perspectives, while the new 2008 version expands these perspectives by adding an integrity and process orientation to the document along a life-cycle compatibility with other standards. This revision of Regulatory Guide 1.170 addresses the expansion of IEEE Std. 829-2008 by updating the existing sections starting with the "Test Program" and then adding 3 new Staff Regulatory Guidance positions to the regulatory guide. In Regulatory Guide 1.170 the "Test Program" in Staff Regulatory Guidance position 1 directs the licensee to use the Master Test Plan (MTP) in IEEE Std. 829-2008, Clause 8, and outlines additional requirements with the associated IEEE Subclauses. The MTP overview provides a method of managing design details for test documentation, while following the life-cycle process and tracking occurrences, and documenting the software corrections, as noted in IEEE Std. 829-2008, Clause 14, Anomaly Report.

Staff Regulatory Guidance position 2 of Regulatory Guide 1.170 has been expanded to include details on the Master Test Report (MTR) and the sequence of other test documents that could occur during a life-cycle process. Because of the integrity scheme level required, the different sequences of test reports are distilled into the summarization MTR. Staff Regulatory Guidance position 3 also includes details for effective document retention which includes ways to combine or eliminate added documents.

The original Staff Regulatory Guidance position 4 in Regulatory Guide 1.170 stated that any given safety system feature is tested formally by a given test design, while other features may be exercised but not identified. With the traceability matrix in Staff Regulatory Guidance position 5 and the expanded test documentation for integrity level 4, there can be multiple sets of design testing or retesting to complete an acceptable safety system or software product. The licensee should formally test all associated features in the safety system and follow the recommended testing activity process outlined under Clause 5 in IEEE Std. 829-2008. As for each specifically planned test, the acceptance criteria requirement is that any testing must show positive results and, if an error exists, the documentation must show the corrections and retesting, as any modified software has the potential of introducing new errors.

The new Staff Regulatory Guidance position 6, "Integrity Levels" introduces an integrity scheme level 4, which is maintained throughout the life-cycle testing process independent of any risk assessment schemes. For level 4 the breadth, depth of testing, and the associated type of tasks can be found in Annex C of IEEE Std. 829-2008, as described in the new Staff Regulatory Guidance position 7, "Testing Tasks." For example: The Level Interim Test Status Report can be used to maintain a time sequence during the project development and assists in the documentation as an output. As the safety analysis activities are being completed, the output requirements should be adequately addressed so that no hazards have been introduced into the final code prior to the V&V testing. The MTP's goal is to address and orchestrate all testing and reporting documentation with positive results.

As automated tools are used for testing software, the new Staff Regulatory Guidance position 8, "Test Tool Documentation" points out that repetition is sometimes needed. There is a need for making test information easily accessible to the NRC staff and thus improving the timeliness of a safety conclusion.

In specific tasks of identifying security issues, the IEEE Std. 829-2008 Std. provides an opportunity to integrate this task within the life-cycle phases, which can be found in Table 3. The secure analysis of any software project is part of the software requirement specification and Annex C of IEEE Std. 829-2008 breaks the inputs down further in system, software, and interface requirements. In Regulatory Guide 1.170, the new Staff Regulatory position 9, "Security Analysis," outlines this additional task, where it should be considered as early as possible in the life-cycle phases. The NRC further

supplements this V&V life-cycle approach by providing secure development and operational environment (SDOE) guidance when developing a digital safety system. To meet the criteria of IEEE Std. 603-1991 and 10 CFR 50, Appendix B, the development of digital safety system software requires a SDOE be provided, Regulatory Guide 1.152, "Criteria for Use of Computers in Safety Systems in Nuclear Power Plants" provides specific guidance concerning the establishment of the 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 that should also be documented; however, a licensee's adherence to the provisions of 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks," (Ref. 15) will be evaluated per regulatory programs specific to that regulation and in accordance with the applicant's NRC-approved cyber security plan. IEEE Std. 829-2008 is not endorsed in this regulatory guide as being appropriate for compliance with 10 CFR 73.54.

This regulatory guide is based on standards and describes methods acceptable for any safety system software and discusses the required test documentation 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 regulatory guide, IAEA Safety Guide NS-G-1.1, "Software for Computer Based Systems Important to Safety in Nuclear Power Plants" issued September 2000 (Ref. 16) discusses the importance of documentation for computer software used in safety related systems. This regulatory guide incorporates similar documentation 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 approval as an acceptable approach for meeting an NRC requirement. However, licensees and applicants may consider and use the information in the secondary reference, if appropriately justified and consistent with current regulatory practice, consistent with applicable NRC requirements.

C. STAFF REGULATORY GUIDANCE

IEEE Std. 829-2008 provides an acceptable approach to the NRC for meeting the agency's regulatory requirements on the test documentation of safety system software with the exceptions and additions listed in these regulatory positions. The annexes to IEEE Std. 829-2008 contain information

that may be useful; however, 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. In this section of the guide, the cited criteria refers to Appendix B to 10 CFR Part 50 unless otherwise noted.

1. Test Program

IEEE Std. 829-2008 does not mandate the use of all its software and system test documentation in any given test phase; instead, it recommends, as best practices, the use of the integrity level scheme and the life-cycle processes for the appropriate test activities and tasks that result in the needed test documentation. If the licensee chooses a subset of the IEEE Std. 829-2008 documentation for a particular test phase, it should include the information necessary to meet the regulatory requirements on software and system test documentation. The subset should demonstrate minimum testing tasks for the designated integrity level in conjunction with each associated life-cycle phase and documented to the highest level of documentation in the Clause 8, MTP, and the highest level selected test documentation from Clause 9 through Clause 17. The MTP is also called upon to follow, with the associated Clauses 9 through 17, the life-cycle test processes found in Clause 5, which further outlines in IEEE Std. 829-2008, Table 3 the required testing activities based upon the integrity level.

With an integrity level 4, Table 2 in IEEE Std. 829-2008 calls for the use of the MTP and associated documents. As a minimum, the information additions highlighted below with the MTP, provides an acceptable approach for the licensee to plan the test document tasks and activities, and thus to adequately address the system safety requirements:

a. The qualifications, duties, responsibilities, and skills required of persons and organizations assigned to testing activities has been outlined in Clause 8, while further training may be required, which can be supported by the Level Test Plan (LTP) documentation found under Clause 9.3.6.

b. The refinement of test items, the approach taken by the testing program, and acceptance criteria are outlined in LTP, Clause 9.1.5.

c. The additional information on environmental conditions and special controls, equipment, tools, and instrumentation needed for accomplishing the testing can also be supplemented under the LTP within Clause 9.3.2 and the Level Test Design (LTD), Clause 10.2.2.

d. The documentation topics for system, software, and hardware test instructions and procedures that incorporate the requirements and acceptance limits in applicable design documents have supporting information found in the LTD. The Level Test Case (LTC) outlines further the acceptance criteria under Clause 11.2.5/6, while the steps to be taken in procedure documentation are part of the Level Test Procedure (LTPr), Clause 12.2.2.

e. The additional information on test prerequisites and the criteria for meeting these requirements and acceptance limits is supplemented under LTPr, Clause 12.2.1.

f. The Level Test Log (LTL), Clause 13.2.1 provides further details on test logs and test records that indicate the identity of the tester, the type of observation made, the results / acceptability, and the action taken in connection with any deficiencies.

g. Additional direction for documents, such as test data, and interim reporting test results can be found in the Level Test Log (LTL), Clause 13. The life-cycle processes should

demonstrate adequate testing and error resolution documentation with retesting, which is sustained by an Anomaly Report (AR), Clause 14.

The licensee should incorporate the information items listed above with the normal outline provided in the MTP. The overall test documentation should provide an overview history that the software safety analysis and its test tasks and activities have been successfully completed.

2. Software Documentation

Criteria VI and XVII and 10 CFR 21.51, "Maintenance and Inspection of Records," require the retention of documents and records that affect quality. Because design control measures must be applied to acceptance criteria for tests and because some software and system test documentation is reused and evolves during the course of software development and software maintenance (e.g., regression test documentation), such test documentation should be controlled as one or more configuration items under an SCM system. The licensee must maintain test records, such as test reports, as quality records, and the SCM system should control these records.

Section 5.11(5) of IEEE Std. 603-1991 and Section 4.22 of IEEE Std. 279-1971 require the licensee to distinctly identify documentation, including test records, associated with safety systems. In IEEE Std. 829 the MTP identifies several documents such as LTLs, ARs, Level Interim Test Status Reports (LITSR), Level Test Reports (LTR) and the Master Test Report (MTR). The MTR shall provide information on the summary of testing activities, test task results, anomalies and resolutions, the quality and the final metrics collected. The document should detail the suitability and sustainability of the project and reflect the MTP. Any variations need to follow an established deviation policy as discussed in Clause 8.2.3.3.

3. Test Documentation

Clause 7 of IEEE Std. 829-2008 describes software and system test documentation as a set of individual documents. There are different types and levels of test documentation addressed from Clause 8 through Clause 17, which may be combined or eliminated per Clause 6. For each type of test documentation the licensee must document the software and system test content decisions and rationale at the highest level of testing, and the documentation must be signed-off by all designated stakeholders. It is the NRC's position that, in order to claim conformance to IEEE Std. 829-2008, the documentation should be completed prior to implementation.

For effective document retention, it is acceptable to combine documents by incorporating individual documents into larger test documents, provided that it retains the identity of each component document and maintains the proper test planning documentation throughout the life-cycle process for a proper traceability matrix in V&V. However, it is not acceptable to lower the integrity level as suggested in Clause 6.4, "Choose to combine or eliminate documents."

Furthermore, some acceptance test procedures may have an open entry location within the document, appendix or attachment to record the data and testing status. To meet the activity and event entry per Clause 13, "Level Test Log," an acceptable method for eliminating or combining test documents is to use the procedure and log as the same document (e.g., Factory Acceptance Test Procedures). This is also the case when the test log is the appendix or attachment to the test procedure, and where the procedure is repeated many times (e.g., surveillance procedures).

4. System Testing

Criterion XI requires that testing demonstrate systems and components will perform satisfactorily in service. Clause 10.2.1 (LTD Section 2.1) "Features to be tested" of IEEE Std. 829-2008 describes other features in a given test design and not the specific LTD objective that may be exercised but not identified. The licensee should formally test all associated features in the safety system and follow the recommended testing activity process outlined under Clause 5. Furthermore other testing examples can be found in Clause 9, which may derive more than one testing level per example; e.g., recovery processing software has a normal and failure recovery testing level.

A normal or failure recovery would happen above the unit and either at a component or the system level testing and should be included as a test requirement. In many cases a system's transaction decisions may not find the normal return path, and whether the failure with system software or hardware is initiated by control flow or data flow, a traceable baseline for the failure recovery software testing should be included in the LTD and LTP.

5. Traceability

Criterion XI requires that testing demonstrate that systems and components will perform satisfactorily in service. Traceability analyses relating functions and test cases provide a means for ensuring that all functions are tested (IEEE Std. 1012-2004). The planning for software V&V addresses these analyses. Clause 8.1.3 of IEEE Std. 829-2008 requires that the applicants and licensees list all applicable reference documentation as part of the life-cycle process and with the concerning test documentation derived from Clause 8 through Clause 17. The test documentation from Clause 8 through Clause 17 should include these references unless the licensee maintains equivalent traceability information elsewhere in the V&V records.

6. Integrity Levels

Clause 4 of IEEE Std. 829-2008 defines a four-level method of quantifying software integrity levels in which Level 4 is the highest and Level 1 is the lowest. The standard requires the applicant or licensee to either use the method in the standard or define another method and provide a mapping between its method and the method defined in the standard.

The NRC staff takes exception to the Table B.3, "Risk assessment scheme" in Annex B. The IEEE Std. 829-2008 statement about the Table B.3 illustration for determining the likelihood and evaluating software integrity level lower than Level 4 is not acceptable. 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, as defined in IEEE Std. 829-2008.

7. Testing Tasks

Clause 5 of IEEE Std. 829-2008 lists the minimum testing tasks for each life-cycle process steps that the applicant or licensee may use for the preparation of the required test plans. Table C.1, "Testing tasks, inputs and outputs" per Annex C of IEEE Std. 829-2008 outlines Clause 5 in a tabular form and amplifies the requirements given in the body of the standard by detailing, for each process, the tasks that the licensee and applicant should carry out, as noted under column names "Testing tasks," "Inputs" and "Outputs." For software used in the safety systems of nuclear power plants, applicants and licensees should consider the recommendations in this Annex.

8. Test Tool Documentation

Clause 6.3 of IEEE Std. 829-2008 states that there is no need for repetition of test information if completely managed by an automated tool with references for tracing the information. The NRC staff takes exception to this Clause as there are particular cases where electronic validation methods with repetition provide test information easily accessible for the basis of any safety conclusion. This test information should be available within the record management system. The tools used in the development of safety system software should be handled according to IEEE Std. 7-4.3.2-2003, as endorsed by Regulatory Guide 1.152.

9. Secure Analysis

IEEE Std. 829-2008, Clause 5 and Table 3 list "Identifying security issues (test)" as a required test effort task in the development life-cycle process and only as a minimum recommended test activity covered in the life-cycle areas of "Requirements", "Design," "Implementation," "Test," "Installation/ Checkout," and "Operation Test." The identification of the security issues task should be included in the process activities of "Acquisition," "Supply," "Planning," and "Concept" life-cycle phases in Table 3 and Clause 5.

10. Annexes

IEEE Std. 829-2008 includes the eight informative annexes listed below. These annexes are listed here as sources of information, they are not endorsed by this RG unless otherwise noted:

(1) Annex A, "Bibliography," lists IEEE and International Standardization Organization/ International Electrotechnical Commission (ISO/IEC) standards that are useful in implementing and interpreting the test requirements in IEEE Std. 829-2008. Although the NRC does not endorse this annex, applicants and licensees may find it useful.

(2) Annex B, "Example Integrity Level Scheme," is endorsed by this regulatory guide, as described and with the exceptions noted in Staff Regulatory Guidance position 6.

(3) Annex C, "Testing Tasks," is endorsed by this regulatory guide, as described in Staff Regulatory Guidance position 7.

(4) Annex D, "Optional Testing Tasks," describes additional testing tasks that may be performed. Although the NRC does not endorse this annex, applicants and licensees may find it useful.

(5) Annex E, "Metrics from a Test Management Perspective," describes briefly the concept of testing metrics and provides an outline for a metrics report. Although the NRC does not endorse this annex, applicants and licensees may find it useful.

(6) Annex F, "Independence," very briefly discusses the independence of testing groups from development groups. Although the NRC does not endorse this annex, applicants and licensees may find it useful.

(7) Annex G, "Examples of Tailoring Documentation Contents," describes how other software documentation may cover various testing documents, such as configuration management documentation, project plans, and quality assurance and development documents. The NRC does not endorse this annex because it provides examples instead

of regulatory guidelines. The NRC permits the repackaging of document contents, as described here, provided that no information is lost.

(8) Annex H, "Guidelines for Compliance with IEEE/EIA Std. 12207.1-1997," is not endorsed by the NRC because the staff has not reviewed 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. 17) for endorsement.

D. IMPLEMENTATION

The purpose of this section is to provide information on how applicants and licensees[2] may use this guide and information regarding the NRC's plans for using this regulatory guide. In addition, it describes how the NRC 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 regulatory guide may be deemed acceptable if they provide sufficient basis and information for the NRC 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 for complying with the identified regulations as long as their current licensing basis remains unchanged.

Licensees may use the information in this regulatory guide for actions which 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 regulatory guide or applicable parts to resolve regulatory or inspection issues.

Additionally, an existing applicant may be required to comply to new rules, orders, or guidance if 10 CFR 50.109(a)(3) applies.

If a licensee believes that the NRC is either using this regulatory guide or requesting or requiring the licensee to implement the methods or processes in this regulatory guide 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. 18) and the NRC Management Directive 8.4, "Management of Facility-Specific Backfitting and Information Collection" (Ref 19).

Use by NRC Staff

The NRC staff does not intend or approve any imposition or backfitting of the guidance in this regulatory guide. The NRC staff does not expect any existing licensee to use or commit to using 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" means 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.

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

During regulatory discussions on plant specific operational issues, the staff may discuss with licensees various actions consistent with staff positions in this regulatory guide, 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 regulatory guide are part of the licensing basis of the facility. However, unless this regulatory guide 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 regulatory guide constitutes a violation.

If an existing licensee voluntarily seeks a license amendment or change and (1) the NRC staff's consideration of the request involves a regulatory issue directly relevant to this new or revised regulatory guide and (2) the specific subject matter of this regulatory guide 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 regulatory guide or provide an equivalent alternative process that demonstrates compliance with the underlying NRC regulatory requirements. This 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.

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

5. CFR, "Maintenance and Inspection of Records," Section 51, Part 21, Chapter 1, Title 10, "Energy."

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," U.S. NRC: Washington, DC, March 2007.

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

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

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

10. 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.

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

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

13. IEEE, Std. 610.12-1990, "IEEE Standard Glossary of Software Engineering Terminology," Piscataway, NJ, 1990.

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

---

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.

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

16. 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]

17. 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," April 1998, Piscataway, NJ.[7]

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

19. NRC, Management Directive 8.4, "Management of Facility-Specific Backfitting and Information Collection," NRC, 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 0947, by E-mail at sales@iso.org, or on-line at the ISO Store Web site: http://www.iso.org/iso/store.htm.