U.S. NUCLEAR REGULATORY COMMISSION

September 1997

REGULATORY GUIDE

OFFICE OF NUCLEAR REGULATORY RESEARCH

REGULATORY GUIDE 1.169

(Draft was DG–1055)

CONFIGURATION MANAGEMENT PLANS FOR DIGITAL COMPUTER SOFTWARE USED IN SAFETY SYSTEMS OF NUCLEAR POWER PLANTS

A. INTRODUCTION

In 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," paragraph 55a(a)(1) requires, in part, that systems and components be designed, tested, and inspected to quality standards commensurate with the safety function to be performed.[1] Criterion 1, "Quality Standards and Records," of Appendix A, "General Design Criteria for Nuclear Power Plants," of 10 CFR Part 50 requires, in part,[1] that appropriate records of the design and testing of systems and components important to safety be maintained by or under the control of the nuclear power unit licensee throughout the life of the unit. Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," to 10 CFR Part 50 describes criteria that must be met by a quality assurance program for systems and components that prevent or mitigate the consequences of postulated accidents. In particular, besides the systems and components that directly prevent or mitigate the consequences of postulated accidents, the criteria of Appendix B also apply to all activities affecting the safety-related functions of such systems and components, such as designing, purchasing, installing, testing, operating, maintaining, or modifying. A specific requirement is contained in 10 CFR 50.55a(h), which requires that reactor protection systems satisfy the criteria of IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations."[2] Paragraph 4.3 of IEEE Std 279–1971[3] states that quality of components is to be achieved through the specification of requirements known to promote high quality, such as requirements for design, inspection, and test.

Many of the criteria in Appendix B to 10 CFR Part 50 contain requirements closely related to the configuration management activity. Criterion III, "Design Control," of Appendix B requires measures for design documentation and identification and control of design interfaces. The same criterion also requires that design changes be subject to design control measures commensurate with those used in the original design. Criterion VI, "Document Control," requires that all documents that prescribe activities affecting quality, such as

[1]In this regulatory guide, many of the regulations have been paraphrased; see 10 CFR Part 50 for the full text.

[2]Revision 1 of Regulatory Guide 1.153, "Criteria for Safety Systems," endorses IEEE Std 603–1991, "Criteria for Safety Systems for Nuclear Power Generating Stations," as a method acceptable to the NRC staff for satisfying the NRC's regulations with respect to the design, reliability, qualification, and testability of the power, instrumentation, and control portions of the safety systems of nuclear power plants.

[3]IEEE publications may be obtained from the IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854.

USNRC REGULATORY GUIDES

Regulatory Guides are issued to describe and make available to the public such information as methods acceptable to the NRC staff for implementing specific parts of the Commission's regulations, techniques used by the staff in evaluating specific problems or postulated accidents, and data needed by the NRC staff in its review of applications for permits and licenses. Regulatory guides are not substitutes for regulations, and compliance with them is not required. Methods and solutions different from those set out in the guides will be acceptable if they provide a basis for the findings requisite to the issuance or continuance of a permit or license by the Commission.

This guide was issued after consideration of comments received from the public. Comments and suggestions for improvements in these guides are encouraged at all times, and guides will be revised, as appropriate, to accommodate comments and to reflect new information or experience.

Written comments may be submitted to the Rules Review and Directives Branch, DFIPS, ADM, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001.

The guides are issued in the following ten broad divisions:

1. Power Reactors
2. Research and Test Reactors
3. Fuels and Materials Facilities
4. Environmental and Siting
5. Materials and Plant Protection
6. Products
7. Transportation
8. Occupational Health
9. Antitrust and Financial Review
10. General

Single copies of regulatory guides may be obtained free of charge by writing the Printing, Graphics and Distribution Branch, Office of Administration, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001; or by fax at (301)415-5272.

Issued guides may also be purchased from the National Technical Information Service on a standing order basis. Details on this service may be obtained by writing NTIS, 5285 Port Royal Road, Springfield, VA 22161.

instructions, procedures, and drawings, be subject to controls that ensure that documents, including changes, are reviewed for adequacy and approved for release by authorized personnel. Criterion VIII, "Identification and Control of Materials, Parts, and Components," requires, in part, that parts and components be identified to prevent the use of incorrect or defective parts or components. Criterion XVI, "Corrective Action," requires that conditions adverse to quality, such as failures, malfunctions, deficiencies, and others, be identified, and that the cause be determined, the condition be corrected, and the entire process be documented. Criterion XVII, "Quality Assurance Records," requires in part that sufficient records be maintained so that data that is closely associated with the qualification of personnel, procedures, and equipment be identifiable and retrievable.

This regulatory guide, which endorses IEEE Std 828–1990, "IEEE Standard for Software Configuration Management Plans,"[3] and ANSI/IEEE Std 1042–1987, "IEEE Guide to Software Configuration Management,"[3] with the exceptions stated in the Regulatory Position, describes methods acceptable to the NRC staff for complying with the NRC's regulations for promoting high functional reliability and design quality in software used in safety systems.[4] In particular, the methods are consistent with the previously cited General Design Criteria and the criteria for quality assurance programs of Appendix B as they apply to the maintenance of appropriate records of, and control of, software development activities. The criteria of Appendices A and B apply to systems and related quality assurance processes and, if those systems include software, the requirements extend to the software elements.

In general, information provided by regulatory guides is reflected in the Standard Review Plan (NUREG–0800). The Office of Nuclear Reactor Regulation uses the Standard Review Plan to review applications to construct and operate nuclear power plants. This regulatory guide will apply to the revised Chapter 7 of the Standard Review Plan.

The information collections contained in this regulatory guide are covered by the requirements of 10 CFR Part 50, which were approved by the Office of Management and Budget, approval number 3150–0011. The NRC may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number.

B. DISCUSSION

The use of industry consensus 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 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 based on past experience and represent industry consensus on approaches used for development of such systems.

Software incorporated into instrumentation and control systems covered by Appendix B will be referred to in this regulatory guide as safety system software. For safety system software, identification, control, and documentation of the software must be accomplished as part of the effort to achieve compliance with the NRC's requirements. In addition to the record maintenance requirement of Criterion 1 of Appendix A, Appendix B to 10 CFR Part 50 provides detailed quality assurance criteria, including criteria for administrative control, design documentation, design interface control, design change control, document control, identification and control of parts and components, and control and retrieval of qualification information associated with parts and components. For software, these activities are often called, in aggregate, "software configuration management" (SCM). SCM is identified as a safety system criterion by the industry standard, IEEE Std 7–4.3.2–1993, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,"[3] which is endorsed by Revision 1 of Regulatory Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants."

Configuration management is a significant part of high quality engineering activities and is already required by the NRC staff for structures, systems, and components important to safety. While the principles and intentions of traditional configuration management apply equally to software, there is also a significant change in emphasis for which traditional hardware configuration management systems might not be sufficient. This is because with software there is a greater emphasis on design process and the deliverable product is more like a design output. In the production of engineered hardware, design outputs are inputs to a manufacturing process, and configuration management

[4]The term "safety systems" is synonymous with "safety-related systems." The General Design Criteria cover systems, structures, and components "important to safety." The scope of this regulatory guide is, however, limited to "safety systems," which are a subset of "systems important to safety."

activities focus on ensuring that design outputs and manufacturing process variables are traceable to identifiable manufactured products. In contrast, with engineered software, a large amount of design process information and many intermediate design outputs are associated with the final design output. Relatively many software engineering changes are expected and encountered. Consequently, although similar in intent to hardware configuration management, software configuration management requires a change in emphasis, with expansion of the importance of intermediate design baselines and associated design process information. The needs for robust change management and identification and control of product versions are also substantially increased.

One consensus standard on software engineering, IEEE Std 828–1990, "IEEE Standard for Software Configuration Management Plans," and one IEEE guide, ANSI/IEEE Std 1042–1987, "IEEE Guide to Software Configuration Management" (reaffirmed in 1993), describe software industry approaches to SCM that are generally accepted in the software engineering community. They provide guidance for planning and executing an SCM program. Together, this IEEE standard and guide elaborate on the important features required in an SCM program that may be underemphasized in traditional hardware configuration management programs.

The relationship of IEEE Std 1042–1987 to IEEE Std 828–1990 is important. IEEE Std 1042–1987 is a tutorial guide that explains how to comply with IEEE Std 828–1990. Section 1.1, "Scope," of IEEE Std 1042–1987 states that the guide provides suggestions and examples and "presents an interpretation of how IEEE Std 828–1983 [since updated to IEEE Std 828–1990] can be used for planning the management of different kinds of computer program development and maintenance activities." The actual criteria to be met for compliance with the standard are contained in IEEE Std 828–1990. Both the standard and the guide apply to general purpose software development and maintenance efforts, and they do not have specific criteria for safety system software.

C. REGULATORY POSITION

IEEE Std 828–1990, "IEEE Standard for Software Configuration Management Plans," provides an approach acceptable to the NRC staff for meeting the requirements of 10 CFR Part 50, as applied to software, in planning configuration management of safety system software, subject to the provisions listed below.

ANSI/IEEE Std 1042–1987, "IEEE Guide to Software Configuration Management," subject to the provisions listed below, provides guidance acceptable to the NRC staff for carrying out software configuration management plans produced under the auspices of IEEE Std 828–1990. IEEE Std 1042–1987 should be used with the definitions of IEEE Std 828–1990 to implement the details of plans prepared pursuant to IEEE Std 828–1990. In the provisions listed below, reference is made to explanatory sections of IEEE Std 1042–1987 where appropriate to clarify SCM concepts.

To meet the cited requirements of Appendix A to 10 CFR Part 50 by complying with the cited criteria of Appendix B, the following exceptions are necessary and will be considered by the NRC staff in the review of submittals from applicants and licensees. (In this Regulatory Position, the cited criteria are in Appendix B to 10 CFR Part 50 unless otherwise noted.)

1. DEFINITIONS

IEEE Std 828–1990 refers to IEEE Std 610.12–1990, "IEEE Standard Glossary of Software Engineering Terminology," for definitions of the technical terms that are enumerated in section 1.3 of IEEE Std 828–1990. These definitions are acceptable with the following clarifications and additions:

1.1 Baseline

Meaning (1) of baseline is to be used in IEEE Std 828–1990. Formal review and agreement is taken to mean that responsible management has reviewed and approved a baseline. Baselines are subject to change control. Acceptable baseline change approval authority is described in Exception 2 below.

1.2 Promotion

The term "promotion," as defined in Section 1.4 of IEEE Std 1042–1987, is added to the list of defined terms.

1.3 Interface

All four variations of the meaning of interface are to be used in IEEE Std 828–1990, depending upon the context. Meaning (1), "A shared boundary across which information is passed," is interpreted broadly according to Criterion III to include design interfaces between participating design organizations.

1.4 Configuration Audit

IEEE Std 610.12–1990 refers the definition of configuration audit to two other audits without specifying whether one or both definitions are meant. In the

context of an audit for delivery of a product, a configuration audit includes both a functional configuration audit and a physical configuration audit.

2. AUTHORITY LEVELS

Section 2.2.4 of IEEE Std 1042–1987 is modified to permit hierarchies of change approval authority levels, as described in that section and discussed in section 3.3.2.1, provided the required authority level is commensurate with life cycle stage (nearness to release) and product importance to safety. The promotion of a software product might involve a change in level of control and responsible individual.

3. ACCEPTANCE CRITERIA

Criterion II, "Quality Assurance Program," states that activities affecting quality are to be accomplished under suitably controlled conditions. Criterion V, "Instructions, Procedures, and Drawings," states that instructions, procedures, or drawings are to include appropriate quantitative or qualitative acceptance criteria for determining that important activities have been satisfactorily accomplished. Section 1.3 of IEEE Std 828–1990 defines "control point." The software configuration management (SCM) plan should describe the criteria for selecting control points and establish the correspondence between control points identified in the plan and baselines, project milestones, and life cycle milestones.

4. CONFIGURATION MANAGEMENT

Section 2.3 of IEEE Std 828–1990 describes four functional areas under which configuration management activities are grouped: configuration identification, configuration control, status accounting, and configuration reviews and audits. However, while IEEE Std 828–1990 requires that SCM plans describe provisions for these activities, it has no minimal set of activities for safety system software. Criterion II, "Quality Assurance Program," states that activities affecting quality are to be accomplished under suitably controlled conditions. Criteria III, "Design Control"; VI, "Document Control"; VII, "Control of Purchased Material, Equipment, and Services"; VIII, "Identification and Control of Materials, Parts, and Components"; XVII, "Quality Assurance Records"; and XVIII, "Audits," address various aspects of the need for controlling designs, documentation, and materials. For safety system software, the minimal set of activities must accomplish the following: identification and control of all software designs and code, identification and control of all software design interfaces, control of all software design changes, control of software documentation (user, operating, and maintenance documentation), control of software vendors supplying safety system software, control and retrieval of qualification information associated with software designs and code, software configuration audits, and status accounting. Some of these functions or documents may be performed or controlled by other quality assurance activities; in this case the SCM plan should describe the division of responsibility.

5. CORRECTIVE ACTION

Criterion XVI, "Corrective Action," requires that conditions adverse to quality, such as failures, malfunctions, deficiencies, and others, be identified, the cause be determined, the condition be corrected, and the entire process be documented. In software development or maintenance, the responsibility for these activities is often distributed among several organizations, possibly leading to a fragmented view of the correction process. Section 2.3.2 of IEEE Std 828–1990 requires a partial description of the correction process, including change requests, change evaluation, change approval, change implementation, change verification, and changed-version release. The preliminary steps leading to a change request should also be described, including responsibility for executing and documenting anomaly reports, problem analyses, and statistical monitoring of software performance. If these activities are described by other documents, the descriptions may be included by reference.

6. DOCUMENTATION

Section 2.3.1.1 of IEEE Std 828–1990 requires, as a minimum, that all configuration items that are to be delivered be listed in the SCM plan. This fulfills the intent of Criterion VIII, "Identification and Control of Materials, Parts, and Components," with regard to safety system software if all software deliverables are identified and controlled as configuration items. Criterion III, "Design Control," requires measures for design documentation, identification and control of design interfaces, and control of design changes. Criterion VI, "Document Control," requires that all documents that prescribe activities affecting quality, such as instructions, procedures, and drawings, be subject to controls that ensure that documents, including changes, are reviewed for adequacy and approved for release by authorized personnel. Criterion XVII, "Quality Assurance Records," requires in part that sufficient records be maintained so that data that is closely associated with the qualification of personnel, procedures, and equipment will be identifiable and retrievable. This regulatory guide applies to all aspects of the software life cycle within the system life cycle context.

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

- Software requirements, designs, and code
- Support software used in development (exact versions)
- Libraries of software components essential to safety
- Software plans that could affect quality
- Test software requirements, designs, or code used in testing
- Test results used to qualify software
- Analyses and results used to qualify software
- Software documentation
- Databases and software configuration data
- Commercial software items that are safety system software
- Software change documentation

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

7. CONTROL OF PURCHASED MATERIALS

Criterion VII, "Control of Purchased Material, Equipment, and Services," requires measures to ensure that purchased material conforms to procurement documents. Criterion VIII, "Identification and Control of Materials, Parts, and Components," requires measures to be established for the identification and control of materials, parts, and components. Contractually developed or qualified commercial software products that are safety system software must be taken under control by an SCM program that complies with IEEE Std 828–1990 as endorsed by this regulatory guide. This means, for example, that the exact version of the product is identified and controlled according to the change control procedures applied to other configuration items and that its usage is tracked and reported.

8. DEVELOPMENT TOOLS

Tools used in the development of safety system software should be handled according to IEEE Std 7–4.3.2–1993, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," as endorsed by Revision 1 of Regulatory Guide 1.152. In particular, tools must be taken under control (i.e., treated as a configuration item) by an SCM program operated by the using organization that complies with IEEE Std 828–1990 as endorsed by this regulatory guide.

9. ACCEPTANCE CRITERIA

Criterion V, "Instructions, Procedures, and Drawings," requires that instructions, procedures, and drawings include appropriate quantitative or qualitative acceptance criteria for determining that important activities have been satisfactorily accomplished. In addition, Criterion VIII, "Identification and Control of Materials, Parts, and Components," requires measures to be established for the identification and control of materials, parts, and components; and Criterion II, "Quality Assurance Program," states that activities affecting quality must be accomplished under suitably controlled conditions. In order to maintain acceptance criteria established in accordance with Criterion V and suitably controlled conditions (in accordance with Criteria II and VIII) for safety system software, section 3.2 of IEEE Std 828–1990 is not endorsed by this regulatory guide.

10. DESIGN VERIFICATION

IEEE Std 828–1990, in paragraph 2.3.2(4), requires a definition of the verification, implementation, and release of a change. The criteria for verification must be consistent with Criterion III, "Design Control," which requires that design changes be subject to design control measures commensurate with those applied to the original design. This encompasses the re–examination of any appropriate safety analysis related to the change.

11. SCM PLAN

IEEE Std 828–1990, in paragraph 2.1(7), requires the SCM plan to address the assumptions upon which the plan is based, including assumptions that might have an impact on cost and schedule. Any use of cost and schedule criteria must be consistent with the requirement of 10 CFR 50.57(a)(3) that there be reasonable assurance that the activities authorized by the operating license can be conducted without endangering the health and safety of the public.

12. BACKFIT CLARIFICATION

Section 1.1 of IEEE Std 828–1990 states "It also applies to non-critical software and to software already developed." Such statements in the standard should not be interpreted as requirements for backfit. See the Implementation section of this regulatory guide for the NRC staff's position on backfitting regarding this guidance.

13. OTHER CODES AND STANDARDS

IEEE Std 828–1990 and IEEE Std 1042–1987 reference other industry codes and standards. These references to other standards should be treated individually. If a referenced standard has been incorporated separately into the NRC's regulations, licensees and applicants must comply with that standard as set forth in the regulation. If the referenced standard has been endorsed in a regulatory guide, the standard constitutes a method acceptable to the NRC staff of meeting a regulatory requirement as described in the regulatory guide. If a referenced standard has been neither incorporated into the NRC's regulations nor endorsed in a regulatory guide, licensees and applicants may consider and use the information in the referenced standard, if appropriately justified, consistent with current regulatory practice.

D. IMPLEMENTATION

The purpose of this section is to provide information to applicants and licensees regarding the NRC staff's plans for using this regulatory guide. No backfitting is intended or approved in connection with this guide.

Except in those cases in which an applicant or licensee proposes an acceptable alternative method for complying with the specified portions of the NRC's regulations, the methods in this guide will be used in the evaluation of submittals in connection with applications for construction permits and operating licenses. This guide will also be used to evaluate submittals from operating reactor licensees that propose system modifications voluntarily initiated by the licensee if there is a clear nexus between the proposed modifications and this guidance.

BIBLIOGRAPHY

Hecht, H., A.T. Tai, K.S. Tso, "Class 1E Digital Systems Studies," NUREG/CR-6113, USNRC, October 1993.[1]

Institute of Electrical and Electronics Engineers, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," IEEE Std 7-4.3.2, 1993.

Lawrence, J.D., "Software Reliability and Safety in Nuclear Reactor Protection Systems," NUREG/CR-6101 (UCRL-ID-117524, Lawrence Livermore National Laboratory), USNRC, November 1993.[1]

Lawrence, J.D., and G.G. Preckshot, "Design Factors for Safety-Critical Software," NUREG/CR-6294, USNRC, December 1994.[1]

Seth, S., et al., "High Integrity Software for Nuclear Power Plants: Candidate Guidelines, Technical Basis and Research Needs,"[1] NUREG/CR-6263, USNRC, June 1995.[1]

USNRC, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," Regulatory Guide 1.152, Revision 1, January 1996.[2]

USNRC, "Standard Review Plan," NUREG-0800, February 1984.

[1]Copies may be purchased at current rates from the U.S. Government Printing Office, P.O. Box 37082, Washington, DC 20402-9328 (telephone (202)512-2249); or from the National Technical Information Service by writing NTIS at 5285 Port Royal Road, Springfield, VA 22161. Copies are available for inspection or copying for a fee from the NRC Public Document Room at 2120 L Street NW., Washington, DC; the PDR's mailing address is Mail Stop LL-6, Washington, DC 20555-0001; telephone (202)634-3273; fax (202)634-3343.

[2]Single copies of regulatory guides may be obtained free of charge by writing the Office of Administration, Printing, Graphics and Distribution Branch, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001; or by fax at (301)415-5272. Copies are available for inspection or copying for a fee from the NRC Public Document Room at 2120 L Street NW, Washington, DC; the PDR's mailing address is Mail Stop LL-6, Washington, DC 20555-0001; telephone (202)634-3273; fax (202)634-3343.

REGULATORY ANALYSIS

A separate regulatory analysis was not prepared for this regulatory guide. The regulatory analysis prepared for Draft Regulatory Guide DG-1055, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," provides the regulatory basis for this guide. A copy of the regulatory analysis is available for inspection and copying for a fee at the NRC Public Document Room, 2120 L Street NW., Washington, DC; the PDR's mailing address is Mail Stop LL-6, Washington, DC 20555-0001; phone (202)634-3273; fax (202)634-3343.

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, DC 20555-0001

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300

FIRST CLASS MAIL
POSTAGE AND FEES PAID
USNRC
PERMIT NO. G-67

☆ U.S. GOVERNMENT PRINTING OFFICE: 1997 417-801/60036