U.S. NUCLEAR REGULATORY COMMISSION

September 1997

REGULATORY GUIDE

OFFICE OF NUCLEAR REGULATORY RESEARCH

REGULATORY GUIDE 1.173

(Draft was DG–1059)

DEVELOPING SOFTWARE LIFE CYCLE PROCESSES 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,[1] that systems and components be designed, tested, and inspected to quality standards commensurate with the safety function to be performed. Criterion 1, "Quality Standards and Records," of Appendix A, "General Design Criteria for Nuclear Power Plants," to 10 CFR Part 50 requires, in part,[1] that a quality assurance program be established and implemented in order to provide adequate assurance that 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 a quality assurance program for systems and components that prevent or mitigate the consequences of postulated accidents must meet. 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 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 279–1971, "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 testing.

In Appendix B to 10 CFR Part 50, many of the criteria contain requirements closely related to software life cycle activities. Criterion I, "Organization," describes the establishment and execution of a quality assurance program. Criterion II, "Quality Assurance Program," states, in part, that activities affecting quality must be accomplished under suitably controlled conditions, which include assurance that all prerequisites for a given activity have been satisfied. This criterion also

[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.

calls for taking into account the need for special controls and processes to attain the required quality. Criterion III, "Design Control," states, in part, that measures must be established for the identification and control of design interfaces and for coordination among participating design organizations. Criterion XV, "Nonconforming Materials, Parts, or Components," requires measures to be established to control materials, parts, or components that do not conform to requirements in order to prevent their inadvertent use or installation. Finally, Criteria VI, "Document Control," and XVII, "Quality Assurance Records," provide for the control of the issuance of documents, including changes thereto, that prescribe all activities affecting quality and provide for the maintenance of sufficient records to furnish evidence of activities affecting quality.

This regulatory guide endorses IEEE Std 1074–1995, "IEEE Standard for Developing Software Life Cycle Processes,"[3] subject to the exceptions stated in the Regulatory Position. IEEE Std 1074–1995 describes a method acceptable to the NRC staff for complying with parts of the NRC's regulations for promoting high functional reliability and design quality in software used in safety systems.[4] In particular, the method is consistent with the previously cited General Design Criteria and the criteria for quality assurance programs of Appendix B as they apply to software development processes. 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). NRC's 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.

[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."

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. The development of software for high-integrity applications, such as safety system software, requires the use of a carefully planned and controlled development process that incorporates the best available approaches to the various aspects of software engineering. There are a number of consensus standards that provide guidance on implementing currently accepted approaches to specific software engineering activities such as software requirements specification or software configuration management. A carefully planned and controlled software development effort must incorporate these specific activities into an orderly process to be followed in the software life cycle, including pre-software-development and post-software-development processes. This regulatory guide addresses the subject of designing software life cycle processes appropriate for the development of safety system software.

IEEE Std 1074–1995 describes, in terms of inputs, development, verification or control processes, and outputs, a set of processes and constituent activities that are commonly accepted as composing a controlled and well-coordinated software-development process. It describes inter-relationships among activities by defining the source activities that produce the inputs and the destination activities that receive the outputs. The standard specifies activities that must be performed and their inter-relationships; it does not specify complete acceptance criteria for determining whether the activities themselves are properly designed. Therefore, the standard should be used in conjunction with guidance from other appropriate regulatory guides, standards, and software engineering literature. IEEE Std 1074–1995 can be used as a basis for developing specific software life cycle processes that are consistent with regulatory requirements, as applied to software, for controlling and coordinating the design of safety system software.

Software development processes are intimately related to system development processes. In the system design phase, system safety requirements are allocated to hardware, software, and human elements. In the system integration and testing phases, these elements are combined and tested. Consequently, a standard for software development processes is intimately related to system-level standards, such as IEEE Std 7–4.3.2–1993, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," which is endorsed by Revision 1 of Regulatory Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants." IEEE Std 1074–1995 describes a complete set of software life cycle processes; however, its system-level view is a generic view from a software perspective. To employ IEEE Std 1074–1995 for developing safety system software, the system-level activities described in IEEE Std 1074–1995 must be addressed within the context provided by regulation and by nuclear industry standards. Examples of system-level issues from this context are the need for software safety analyses as part of system safety evaluation and the need for determining the acceptability of pre-existing software for use in safety systems. Information on software safety activities and software life cycle activities in general can be found in Revision 1 of Regulatory Guide 1.152; NUREG/CR–6101, "Software Reliability and Safety in Nuclear Reactor Protection Systems"[5] (November 1993); and NUREG/CR–6263, "High Integrity Software for Nuclear Power Plants: Candidate Guidelines, Technical Basis and Research Needs"[5] (June 1995). The second area, the acceptability of pre-existing software, is particularly important in the nuclear context. Guidance on this subject is in Revision 1 of Regulatory Guide 1.152.

C. REGULATORY POSITION

The requirements contained in IEEE Std 1074–1995, "IEEE Standard for Developing Software Life Cycle Processes,"[3] provide an approach acceptable to the NRC staff for meeting the requirements of 10 CFR Part 50 and the guidance in Revision 1 of Regulatory Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," as they apply to development processes for safety system software, subject to the provisions listed below. The appendices to IEEE Std 1074–1995 are not endorsed by this regulatory guide.

To meet the requirements of 10 CFR 50.55a(h) and Appendix A to 10 CFR Part 50 as ensured by complying with the criteria of Appendix B applied to the development processes for safety system software, the following provisions are necessary and will be considered by the NRC staff in the review of applicant submittals. (In this Regulatory Position, the cited criteria are in Appendix B to 10 CFR Part 50 unless otherwise noted.)

1. CLARIFICATIONS

Because IEEE Std 1074–1995 was not written specifically for nuclear safety, the following clarifications apply to the standard.

1.1 Regulatory Requirements Identified

Criterion III, "Design Control," requires measures to ensure that applicable regulatory requirements and the design basis for those structures, systems, and components to which Appendix B applies are correctly translated into specifications, drawings, procedures, and instructions. The descriptions of input information, life cycle activity, and output information that are required by IEEE Std 1074–1995 must identify applicable regulatory requirements, design bases, and related guidance.

1.2 Consistency

Various statements in the standard imply or state that life cycle activities should be consistent with budget and schedule or that contingency actions may be taken to meet schedule or budget (paragraphs 3.2.3 and 3.2.4 of IEEE Std 1074–1995). All such activities and contingency actions must be consistent with and justifiable with 10 CFR 50.57(a)(3), which requires 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.

1.3 Commercial Software

Criterion III, "Design Control," 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. Criterion VII, "Control of Purchased Material, Equipment, and Services," 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. If pre-existing software (i.e., reusable software or commercial off-the-shelf software) is incorporated into a safety system developed under the method de-

[5]Copies are available 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.

scribed by this regulatory guide, an acceptance process must be included at an appropriate point in the life cycle model to establish the suitability of the pre-existing software for its intended use. The acceptance process, its inputs, outputs, activities, pre-conditions, and post-conditions, must meet the applicable regulatory requirements and design bases for the safety system. Revision 1 of Regulatory Guide 1.152 provides information on the acceptance of pre-existing software. Additional detailed information on acceptance processes is available in EPRI TR 106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications" (October 1996).[6]

1.4 Definitions

The following definitions are used in this regulatory guide.

Accident An unplanned event or series of events that result in death, injury, illness, environmental damage, or damage to or loss of equipment or property.

Hazard A condition that is a prerequisite to an accident.

2. COMPLIANCE WITH IEEE Std 1074–1995

Criterion II, "Quality Assurance Program," requires all activities affecting quality to be accomplished under suitably controlled conditions. Section 1.5.1, "Applicability," of IEEE Std 1074–1995 permits elimination of some life cycle activities, although compliance with the standard may not then be claimed. According to this regulatory guide, compliance with IEEE Std 1074–1995 means that all mandatory activities are performed, that the requirements described as 'shall' are met, and that all the inputs, outputs, activities, pre-conditions, and post-conditions mentioned by IEEE Std 1074–1995 are described or accounted for in the applicant's life cycle model. IEEE Std 1074–1995 is an organizing standard that ensures that activities deemed important to software quality are performed and related properly to each other; it does not provide detailed information regarding the implementation of specific life cycle activities.

[6]Electric Power Research Institute documents may be obtained from the EPRI Distribution Center, 207 Coggins Drive, P.O. Box 23205, Pleasant Hill, CA 94523. EPRI TR 106439 is also available for inspection or copying for a fee in 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.

3. SOFTWARE SAFETY ANALYSES

Criterion III, "Design Control," requires measures to ensure that applicable regulatory requirements and the design basis are correctly translated into specifications, drawings, procedures, and instructions. To ensure that safety system software development is consistent with the defined system safety analyses, additional activities beyond those specified in IEEE Std 1074–1995 are necessary. Planned and documented software safety analysis activities should be conducted for each phase of the software development life cycle. Therefore, these analyses should be identified in the applicant's life cycle model, including the following inputs, activity description, and outputs.

3.1 Input Information

- Regulatory requirements and guidance,
- Information reported for the system safety analysis,
- Information from previous phases for the software safety analysis,
- The design information from previous and current system and software phase activities.

3.2 Description

The analyses must ensure that:

- System safety requirements have been correctly addressed,
- No new hazards have been introduced,
- Software elements that can affect safety are identified,
- There is evidence that other software elements do not affect safety, and
- Safety problems and resolutions identified in these analyses are documented.

These activities must be conducted according to a Software Safety Plan addressing the organization to perform the analyses, the responsibilities of its safety officer, the management of the software safety activities, and the analyses to be performed for each phase to address hazards and abnormal conditions and events.

3.3 Output Information

Information for the current phase activities is reported in the software safety analysis. This information should be used for the design activities of the current life cycle phase, subsequent software safety analysis activities, the software configuration management process, and the verification and validation process.

4. NEW OR MODIFIED SAFETY SYSTEM SOFTWARE

Criterion XV, "Nonconforming Materials, Parts, or Components," requires measures to be established to control materials, parts, or components that do not conform to requirements in order to prevent their inadvertent use or installation. The following clarifications should be made to IEEE Std 1074–1995 with respect to the installation and operation of new or modified safety system software.

4.1 Temporary "Work-Around"

In its overview discussion of the "Installation Process," section 6.1.1 of IEEE Std 1074–1995 states: "If a problem arises, it must be identified and reported; if necessary and possible, a temporary 'work-around' may be applied." For the purposes of this regulatory guide, the term 'work-around' is defined as follows.

> A temporary change, to either the software or its configuration, that is made for the purpose of allowing the continuation of installation activities and testing of parts of the software that are unaffected by the temporary change.

4.2 Installation

Installation of new or modified safety system software may only be performed when all functions affected by the software have been declared inoperable according to the plant technical specifications. When software is involved, particularly for distributed software architectures, the determination of affected functions can depend on extremely subtle considerations. An example would be two programs related to each other only through use of a single data item, which might not be evident from the examination of architecture diagrams. As a minimum, all functions performed, in part, by a given software executable should be declared inoperable if the software executable, its configuration, or its operating platform is to be altered; interconnections of all types with other software, hardware, or human elements should also be examined. Any work-arounds employed during installation must be accompanied by a disposition plan, rework procedures that conform to configuration control, verification and validation procedures agreed to under the licensing basis, and a resolution schedule. Before affected functions may be declared operable, the currently approved software, under the control of configuration management, must be installed according to the procedures specified in the installation process. This ensures that the intended software is installed and that any work-arounds employed during the installation activities are removed.

4.3 Operation

Section 6.2.3, "Operate the System," of IEEE Std 1074–1995 requires the identification and reporting of anomalies as well as invocation of the verification and validation (V&V) process and the software configuration management process. Section 6.3, "Maintenance Process," requires the software life cycle to be "remapped and executed, thereby treating the Maintenance Process as iterations of development." This process will produce revisions to software executables and configurations that may then be installed according to the installation process. Maintenance activities must conform to the configuration control and V&V procedures agreed to under the licensing basis.

5. TAILORING SOFTWARE

Criterion V, "Instructions, Procedures, and Drawings," requires that activities affecting quality be prescribed by, and accomplished in accordance with, documented instructions, procedures, or drawings. Section 6.1.5.2 of IEEE Std 1074–1995 permits customer tailoring in the 'Install Software' activity. Any tailoring of packaged software or data in the data base at installation must be consistent with the packaged installation planned information of IEEE Std 1074–1995. Criterion III, "Design Control," requires design changes to be subject to design control measures commensurate with those applied to the original design. Tailoring that constitutes design changes, including configurations not part of the original system design, is not permitted unless such tailoring is subject to the full range of design and quality assurance measures applicable to the development of safety system software.

6. OTHER CODES AND STANDARDS

Various sections of IEEE Std 1074–1995 reference industry codes and standards. These referenced 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 the issuance of this proposed guide.

Except in those cases in which an applicant proposes an acceptable alternative method for complying with the specified portions of the NRC's regulations, the methods described 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 that are 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," 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]

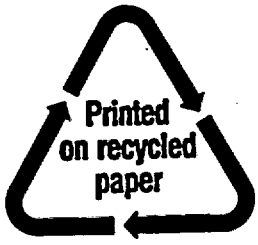
USNRC, "Standard Review Plan," NUREG–0800, February 1984.

[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 Printing, Graphics and Distribution Branch, Office of Administration, 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–1059, "Developing Software Life Cycle Processes 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.



Federal Recycling Program

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 417-801/60040