REGULATORY GUIDE

OFFICE OF NUCLEAR REGULATORY RESEARCH

REGULATORY GUIDE 1.172
(Draft was DG–1058)

SOFTWARE REQUIREMENTS SPECIFICATIONS 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 appropriate records of the design and testing of systems and components important to safety be maintained by or under 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 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 test.

Several of the General Design Criteria (GDC) of Appendix A, including Criteria 12, 13, 19, 20, 22, 23, 24, 25, and 28, describe functions that are part of the design bases of nuclear power plants and that would be included in the software requirements specification (SRS) of any digital computer software that is part of basic components that perform these functions. In addition to the criteria of Appendix A, Appendix B to 10 CFR Part 50 provides quality assurance criteria that

---

[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.

---

design documentation for nuclear reactor safety systems must meet. Criterion III, "Design Control," requires measures for design documentation and identification and control of design interfaces, as well as measures for verifying or checking the adequacy of the design.

This regulatory guide endorses IEEE Std 830-1993, "IEEE Recommended Practice for Software Requirements Specifications,"[3] with the exceptions stated in the Regulatory Position. IEEE Std 830-1993 describes a method acceptable to the NRC staff for complying with the NRC's regulations for achieving high functional reliability and design quality in software used in safety systems.[4] In particular, the method is consistent with GDC 1 and the criteria for quality assurance programs in Appendix B as they apply to the development of software requirements specifications. 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), which is used by the Office of Nuclear Reactor Regulation in the review of applications to construct and operate nuclear power plants. This regulatory guide will apply to the revised Chapter 7 of that document.

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. The software requirements specification is an essential part of the record of the design of safety system software. Associated with system requirements allocated to software subsystems, software requirements serve as the design bases for the software to be developed. Therefore, software requirements specifications are a crucial design input to the remainder of the software development process. Software requirements specifications should exhibit characteristics, such as correctness and completeness, that will facilitate the implementation of a carefully planned and controlled software development process.

One consensus standard on software engineering, IEEE Std 830-1993, describes current practice for writing software requirements specifications for a wide variety of systems. It is not specifically aimed at safety applications; however, it does provide guidance on the development of software requirements specifications that will exhibit characteristics important for developing safety system software. This is consistent with the NRC staff's goals of ensuring high-integrity software in reactor safety systems.

Other standards mention software requirements specifications but do not provide detailed guidance for writing them. 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," mentions unambiguous software requirements as a prerequisite for high quality software development. IEEE Std 1012-1986, "IEEE Standard for Software Verification and Validation Plans,"[3] mentions unambiguous software requirements as a prerequisite for verification and validation. IEEE Std 1074-1991, "IEEE Standard for Developing Software Life Cycle Processes,"[3] describes software requirements specifications as an essential input at the beginning of a software development life cycle. Correct, complete, well-written and unambiguous software requirements are essential inputs to the main design and verification processes that are accepted as necessary to produce high-integrity software products [see NUREG/CR-6101, "Software Reliability and Safety in Nuclear Reactor

---

[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."

Protection Systems" (November 1993),[5] and NUREG/CR-6263, "High Integrity Software for Nuclear Power Plants: Candidate Guidelines, Technical Basis and Research Needs" (June 1995)[5]].

C. REGULATORY POSITION

The recommended practices in IEEE Std 830–1993 provide an approach that is acceptable to the NRC staff for meeting the requirements of 10 CFR Part 50 as they apply to the preparation of software requirements specifications for safety system software, subject to the exceptions listed below.

To meet the requirements of 10 CFR 50.55a(h) and Appendix A to 10 CFR Part 50 as assured by complying with the criteria of Appendix B applied to the verification, validation, reviews, and audits of software used in or affecting basic components of nuclear power plants, 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 A or B of 10 CFR Part 50 unless otherwise noted.)

1. DEFINITIONS

Section 3 of IEEE Std 830–1993 refers to IEEE Std 610.12–1990, "IEEE Standard Glossary of Software Engineering Terminology,"[3] for definitions of technical terms. These definitions are acceptable with the following clarifications or additions.

1.1 Baseline

Meaning 1 of baseline in IEEE Std 610.12–1990 is to be used in IEEE Std 830–1993. Formal review and agreement is taken to mean that responsible management has reviewed and approved a baseline.

1.2 Interface

All four variations of meaning in IEEE 610.12–1990 are to be used in IEEE Std 830–1993, depending on the context. Meaning 1, "A shared boundary across which information is passed," is interpreted broadly according to Criterion III to include design interfaces between participating design organizations.

[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.

2. SOFTWARE REQUIREMENTS SPECIFICATIONS

Section 4.3 of IEEE Std 830–1993 defines a set of characteristics of a good software requirements specification (SRS). The first sentence of this section should be modified to read "An SRS must be...." The following clarifications and additional information should be provided for this set of characteristics for safety system software.

2.1 Traceability and Accuracy

When specification or representation tools are used for requirements, as described in sections 4.3.2.2 and 4.3.2.3 of IEEE Std 830–1993, traceability should be maintained between these representations and the natural language descriptions of the software requirements that are derived from system requirements and system safety analyses.

2.2 Completeness

For safety system software, the description of functional requirements should specify how functions are initiated and terminated as well as the system status at termination. Accuracy requirements, including units, error bounds, data type, and data size, should be provided for each input and output variable. Variables controlled or monitored in the physical environment should be fully described. Functions expressly prohibited should also be described.

Timing information is particularly important in specifying software requirements for safety system software. Functions with timing constraints should be identified and criteria for each mode of operation should be provided. Timing requirements should be deterministic and specified for both normal and anticipated failure conditions.

2.3 Consistency

IEEE Std 830–1993 restricts the term to mean internal consistency, noting that an external inconsistency is actually an incorrect specification of a requirement. The term is used in this regulatory guide to mean both internal and external consistency. External consistency implies that the SRS is consistent with associated software products and system products, such as safety system requirements and design. Internal consistency means that no requirement in the requirements specification conflicts with any other requirement in the specification.

2.4 Ranking for Importance or Stability

For safety system software, this characteristic means that software requirements important to safety must be identified as such in the SRS. Criterion 20 of

Appendix A, among others, describes the functions that reactor protection systems must perform. Section 4.3.5.2 of IEEE Std 830-1993 suggests three degrees of necessity of requirement: *essential, conditional,* and *optional.* As used in IEEE Std 830-1993, the terms conditional and optional refer to requirements that are not necessary for the software to be acceptable. For safety system software, unnecessary requirements should not be imposed. There may be documented variations in essential requirements, but the variations must be linked in the software requirements specifications either to site and equipment variations or to specific plant design bases and regulatory provisions.

2.5 Verifiability

IEEE Std 830-1993 recommends the removal or revision of unverifiable requirements. This is clarified to mean that all requirements should be verifiable and should be modified or restated as necessary so that it is possible to verify each one.

2.6 Modifiability

This term is closely related to the style (form, structure, and modularity), readability, and understandability of the SRS. With respect to these characteristics, it is important that precise definitions of technical terms be available, either in the SRS or in a glossary.

2.7 Traceability

Section 4.3.8 of IEEE Std 830-1993 describes two types of traceability, and both types are required. Each identifiable requirement in an SRS must be traceable backwards to the system requirements and the design bases or regulatory requirements that it satisfies. Each identifiable requirement should be written so that it is also "forward traceable" to subsequent design outputs, e.g., from SRS to software design and from software design to SRS.

Forward traceability to all documents spawned by the SRS includes verification and validation materials. For example, a forward trace should exist from each requirement in the SRS to the specific inspections, analyses, or tests used to confirm that the requirement has been met.

3. CHANGE CONTROL IN SRSs

Section 4.5(b) of IEEE Std 830-1993 recommends that SRSs be baselined and subject to a formal process for control of changes. The SRS must be subject to control of changes. Although this could be met directly by a change control procedure unique to IEEE Std 830-1993, it may also be accomplished by taking the SRS

under a general software configuration management program as a configuration item.

4. INCOMPLETE SRS ENTRY

Any entry in an SRS that is incomplete (uses "TBD"), as described by section 4.3.3.1 of IEEE Std 830-1993, must describe the applicable design bases and commitments to standards or regulations that govern the final determination of the requirement entry.

5. DESIGN-SPECIFIC ISSUES

Section 4.7 of IEEE Std 830-1993 recommends that design-specific issues such as module partitioning, function allocation, and information flow be omitted from SRSs. Section 4.7.1 of IEEE Std 830-1993 states some exceptions to this policy, including reasons of security or safety. When specific design techniques or features such as independence, separation, diversity, and defense-in-depth are required by the safety system design bases or by regulation, these are an appropriate part of an SRS and they should be described therein.

6. SOFTWARE ATTRIBUTES

Section 5.3.6 of IEEE Std 830-1993 lists software attributes that can serve as requirements. Attributes of particular interest for safety system software are safety, security, and reliability or robustness.

6.1 Safety

Software requirements important to safety are derived from system requirements and safety analyses and should be identified as such in the SRS. These requirements should include considerations based on the safety analysis report (SAR) as well as abnormal conditions and events (ACEs) as described in IEEE Std 7-4.3.2-1993, as endorsed by Revision 1 of Regulatory Guide 1.152.

6.2 Security

Security threats to the computer system should be identified and classified according to impact on safety and likelihood of occurrence. Actions required of the software to detect, prevent, or mitigate such security threats should be specified, including access control restrictions. For instance, modification of instrument calibration data might be protected by a password system.

6.3 Robustness

Software requirements for fault tolerance and failure modes, derived either from consideration of system level hazards analyses or from consideration of software internals, should be specified for each operating mode. Software behavior in the presence of unexpected, incorrect, anomalous, and improper input,

hardware behavior, or software behavior should be fully specified. Software requirements for responding to both hardware and software failures should be provided, including requirements for analysis of and recovery from computer system failures. Requirements for on-line in-service testing and diagnostics should be specified.

7. NONAPPLICABILITY

Because of its generality, IEEE Std 830–1993 discusses or recommends a number of content items that may be inappropriate to real-time, embedded safety systems. Headings for such inappropriate subjects in an SRS that is compliant with IEEE Std 830–1993 should be listed, followed by "Not applicable." For example, a graphical user interface may be inappropriate for a real-time, embedded reactor trip system.

8. APPLICABILITY OF ANNEX A

Annex A to IEEE Std 830–1993 is not endorsed by this regulatory guide and may be taken only as examples. Directions to use an outline from Annex A, such as those directions found in section 5.3.7 of IEEE Std 830–1993, may be taken as advisory only.

9. OTHER CODES AND STANDARDS

Various sections in IEEE Std 830–1993 reference several industry codes and standards. These referenced standards should be considered 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 voluntarily initiated by the licensee if there is a clear connection 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.

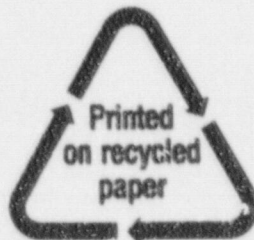[2]Single copies of regulatory guides may be obtained free of charge by writing the Office of Administration, Printing, Graphics and Distribution Branch, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001; or by fax at (301)415–5272. Copies are available for inspection or copying for a fee 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-1058, "Software Requirements Specifications 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.