REGULATORY ANALYSIS

DRAFT REGULATORY GUIDE DG-1209
Software Requirement Specifications for Digital Computer Software used in Safety Systems of Nuclear Power Plants

(Proposed Revision 1 of Regulatory Guide 1.172, dated September 1997)

1. Statement of the Problem

Because traditional and well-understood methods of design and quality assurance for developing and manufacturing hardware apply imperfectly to software design and development, additional guidance beyond standard approaches for hardware is necessary to achieve the intent of U.S. Nuclear Regulatory Commission (NRC) regulations. Many industries that replace traditional hardware-only instrumentation and control (I&C) designs with computers and software are facing this problem. To this extent, the nuclear industry is not very different from any industry associated with high-consequence hazards. Although additional guidance is necessary to help prevent digital I&C safety system failures, the potential benefits of these systems make their use highly desirable.

The use of computers and software in safety-related I&C designs is both part of the larger problem of ensuring the long-term safety of nuclear power plants and part of the solution. It is not just digital systems themselves that raise concerns about design verification and quality assurance; the increase in the complexity of the system designs (including software) being attempted is also a factor. The NRC staff discussed its concerns in SECY-91-292, "Digital Computer Systems for Advanced Light-Water Reactors," dated September 26, 1991 (Ref. 1), and again in parts of SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," dated April 2, 1993 (Ref. 2).

Subsequently, the NRC sponsored studies that resulted in the characterization of design factors, guidelines, technical bases, and practices generally considered appropriate for safety-related software. (See NUREG/CR-6101, "Software Reliability and Safety in Nuclear Reactor Protection Systems," issued November 1993 (Ref. 3); NUREG/CR-6113, "Class 1E Digital Systems Studies," issued October 1993 (Ref. 4); NUREG/CR-6263, "High Integrity Software for Nuclear Power Plants: Candidate Guidelines, Technical Basis, and Research Needs," issued June 1995 (Ref. 5); NUREG/CR-6293, "Verification and Validation Guidelines for High Integrity Systems," issued March 1995 (Ref. 6); and NUREG/CR-6294, "Design Factors for Safety-Critical Software," issued December 1994 (Ref. 7).) These studies identified software design control techniques that are currently being used in "best practice" software development efforts. Although it is possible to simply list the criteria covered, reaching a common understanding between the NRC staff and industry practitioners on what constitutes acceptable software engineering practices for safety systems still remains a problem. An agreed-upon collection of standards, established practices, and engineering techniques for software engineering methods is necessary to complement the collection that already supports traditional hardware engineering methods, such as statistical quality control, testing standards, and quality assurance techniques used on design and manufacturing processes for hardware components.

Software requirement specifications (SRSs) are fundamental to the assurance of software quality, as shown by the large body of literature on the subject. An effective SRS depends on careful planning and execution. For systems and components under its purview, Criterion III, "Design Control," of Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," to Title 10 of the *Code of Federal Regulations*, Part 50, "Domestic Licensing of Production and Utilization Facilities" (10 CFR Part 50), requires licensees to translate applicable regulatory requirements and the

design basis into specifications in design documents. For software systems, the relevant documents include an SRS.

The current industry standard, which is a consensus revision of the standard that Revision 0 of this guide endorses, has captured subsequent experience with SRSs. Consequently, Revision 0 of this guide may not reflect current best practices. In addition, the regulatory framework described in Revision 0 of this guide does not include recent additions to the NRC regulations that apply to new plant licensing.

Therefore, revision of this regulatory guidance is necessary to address the most recent Institute of Electrical and Electronics Engineers (IEEE) standards on the development of an SRS and to incorporate changes to the regulatory framework for new nuclear power plants.

2. Objective

The objective of this regulatory action is to ensure that safety is promoted through effective regulatory guidance that endorses safe practices enhanced through experience, as captured in current consensus standards.

3. Alternative Approaches

The NRC staff considered the following alternative approaches:

Do not revise Regulatory Guide 1.172.
Revise Regulatory Guide 1.172.

Alternative 1: Do Not Revise Regulatory Guide 1.172

Under this alternative, the NRC would not revise this guidance, and the current guidance would be retained. If the NRC does not take action, there would not be any changes in costs or benefit to the public, licensees, or the NRC. However, the "no-action" alternative would not address identified concerns with the current version of the regulatory guide. The NRC would continue to review each application on a case-by-case basis. This alternative provides a baseline condition from which any other alternatives will be assessed.

The impact associated with not revising the regulatory guide to endorse IEEE Standard (Std.) 830-1998, "IEEE Recommended Practice for Software Requirements Specifications," issued 1998 (Ref. 8), is that the NRC and its licensees and applicants may have different interpretations of what constitutes a proper SRS. Failure to revise the regulatory guide does not reduce regulatory uncertainties with respect to SRSs as the NRC staff and its licensees and applicants try to reconcile variations in the descriptions of the regulatory framework and in the usage of multiple versions of industry standards, partly because the current version of the regulatory guide does not address numerous changes in the regulatory environment as follows:

- The NRC has incorporated IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," issued 1991, into 10 CFR 50.55a(h).

- The NRC has added new security requirements to 10 CFR Part 73, "Physical Protection of Plants and Materials," including cyber-security requirements (10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks").

- IEEE has updated IEEE Std. 7-4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," issued 2003, and Regulatory Guide 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," endorses the updated version.

The NRC has updated or is updating other software engineering regulatory guides in parallel with this revision, including Regulatory Guide 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Ref. 9); Regulatory Guide 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Ref. 10); Regulatory Guide 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Ref. 11); Regulatory Guide 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Ref. 12); and Regulatory Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Ref. 13).

Alternative 2: Revise Regulatory Guide 1.172

Under this alternative, the NRC would revise Regulatory Guide 1.172, taking into consideration the enhanced consensus practices for SRSs as embodied in the current version of IEEE Std. 830-1998. Revising the guide would clarify the NRC's position within the regulatory framework and would maintain the set of software engineering regulatory guides as a self-consistent whole. Revising Regulatory Guide 1.172 to maintain consistency with the related requirements and guidance (1) will simplify the staff's review process and enable licensees and applicants to develop a unified, coherent means of meeting the requirements in 10 CFR Part 50 and 10 CFR Part 73 and (2) will reduce regulatory uncertainty and thereby help to minimize the costs associated with the implementation of this guide.

Conclusion

Based on this regulatory analysis, the NRC staff recommends revision of Regulatory Guide 1.172. The staff concludes that the proposed action will enhance reactor safety by providing clear guidance for planning SRSs. The revision of this guide could also reduce regulatory uncertainties and thereby minimize the costs for the industry, especially with regard to applications for standard plant design certifications and combined licenses.

REFERENCES[1]

1. U.S. Nuclear Regulatory Commission (NRC), SECY 91-292, "Digital Computer Systems for Advanced Light-Water Reactors," U.S. NRC, Washington, DC, September 26, 1991. (ADAMS Accession number ML051750018)

2. NRC, SECY 93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," U.S. NRC, Washington, DC, April 2, 1993. (ADAMS Accession Number ML003708021)

3. NRC, NUREG/CR-6101 "Software Reliability and Safety in Nuclear Reactor Protection Systems," U.S. NRC, Washington, DC, November 1993.

4. NRC, NUREG/CR-6113, "Class 1E Digital Systems Studies," U.S. NRC, Washington, DC, October 1993.

5. NRC, NUREG/CR 6263, "High Integrity Software for Nuclear Power Plants: Candidate Guidelines, Technical Basis, and Research Needs," U.S. NRC, Washington, DC, June 1995.

6. NRC, NUREG/CR 6293, "Verification and Validation Guidelines for High Integrity Systems," U.S. NRC, Washington, DC, March 1995.

7. NUREG/CR-6294, "Design Factors for Safety-Critical Software," U.S. Nuclear Regulatory Commission, Washington, DC, December 1994.

8. Institute of Electrical and Electronic Engineers (IEEE) Std. 830-1998, "IEEE Recommended Practice for Software Requirements Specifications," IEEE, Piscataway, NJ, 1998.[2]

9. NRC, Regulatory Guide 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," U.S. NRC, Washington, DC.

10. NRC, Regulatory Guide 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," U.S. NRC, Washington, DC.

11. NRC, Regulatory Guide 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," U.S. NRC, Washington, DC.

12. NRC, Regulatory Guide 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," U.S. NRC, Washington, DC.

---

[1] 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.

[2] Copies of IEEE documents may be purchased from the Institute of Electrical and Electronics Engineers Service Center, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855 or through the IEEE's public Web site at http://www.ieee.org/publications_standards/index.html.

13. NRC, Regulatory Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," U.S. NRC, Washington, DC.