REGULATORY ANALYSIS

DRAFT REGULATORY GUIDE DG-1206

(Proposed Revision 1 of Regulatory Guide 1.169, dated September 1997)

Configuration Management Plans for Digital Computer Software used in Safety Systems of Nuclear Power Plants

Pre-Decisional

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 the 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 failures of digital I&C safety systems, 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 used in "best practice" software development efforts. They resulted in an agreed-upon collection of standards, established practice, and engineering techniques for software engineering methods to complement the collection that already supports traditional hardware engineering methods, such as statistical quality control, testing standards, and quality assurance techniques applied to design and manufacturing processes for hardware components.

Software configuration management (SCM) is fundamental to the assurance of software quality, as evidenced by industry practices and the large body of literature on the subject. An effective SCM program depends on careful planning and execution. These, in turn, depend on appropriate documentation. For systems and components under its purview, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," to Title 10 of *the Code of Federal Regulations* (10 CFR) Part 50, "Domestic Licensing of Production and Utilization Facilities" (Ref. 8), requires design control, including the use of written design control procedures for identifying, controlling, releasing, delivering, and managing software, plus sufficient records to furnish evidence of activities affecting quality. The studies cited above stress the importance of SCM in the development of safety-

related software. NUREG/CR-6101, in its description of activities and related documents necessary for the production of reliable software, addresses SCM. The NRC developed this regulatory guide to ensure that the staff and applicants share a common understanding of an acceptable method for accomplishing SCM.

The current industry standard, which is a consensus revision of the standard endorsed in Revision 0 of this guide, has captured subsequent experience with SCM. Consequently, the present revision of this regulatory guide may not reflect current best practices. In addition, the regulatory framework described in Revision 0 of the 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 revision of Institute of Electrical and Electronics Engineers (IEEE) Standard (Std.) 828-2005, "IEEE Standard for Software Configuration Management Plans," issued 2005, and to incorporate changes to the regulatory framework for new nuclear power plants.

2. Objectives

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 1.169.
Revise Regulatory Guide 1.169.

Alternative 1: Do Not Revise Regulatory Guide 1.169

Under this alternative, the NRC would not revise this guidance, and the current version of this regulatory guide would be retained. If the NRC does not take action, there would be no 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 Std. 828-2005 is that the NRC and its licensees and applicants may have different interpretations of the types and amount of SCM activities necessary to properly plan SCM. The current version of the regulatory guide endorses American National Standards Institute (ANSI)/IEEE Std. 1042-1987, "IEEE Guide to Software Configuration Management," issued 1987 (Ref. 9). This standard is not consistent with IEEE Std. 828-2005, and IEEE has withdrawn it. The current version of the regulatory guide does not address SCM considerations with regard to release management and delivery as well as cyber security. Retaining the current version of the regulatory guide does not reduce regulatory uncertainties with respect to SCM as the NRC staff, licensees, and applicants try to reconcile variations in descriptions of the regulatory framework, as well as the usage of multiple versions of industry standards. In part, this may occur because the current version of regulatory guide does not address numerous changes in the regulatory environment:

Pre-Decisional

- 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 amended 10 CFR Part 73, "Physical Protection of Plants and Materials" (Ref. 10), to add new security requirements, including for cyber security (10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks").

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

- The NRC has updated the other regulatory guides related to software engineering or is updating them in parallel with this revision. These include Regulatory Guide 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants" (Ref. 11); Regulatory Guide 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Ref. 12); Regulatory Guide 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Ref. 13); Regulatory Guide 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Ref. 14); Regulatory Guide 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Ref. 15); and Regulatory Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Ref. 16).

Alternative 2: Revise Regulatory Guide 1.169

Under this alternative, the NRC would revise Regulatory Guide 1.169, taking into consideration the enhanced consensus practices for planning SCM as embodied in the current version of IEEE Std. 828-2005. The review guidance contained in Chapter 7, "Instrumentation and Controls," of NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition" (Ref. 17), also addresses the implementation of those processes.

Revising Regulatory Guide 1.169 will (1) simplify the staff's review process and enable licensees and applicants to develop a unified, coherent means of meeting the requirements of 10 CFR Part 50 and 10 CFR Part 73 and (2) reduce regulatory uncertainty and thereby help to minimize the costs associated with the implementation of this guide.

A benefit of this action is that it would enhance reactor safety by ensuring that clear guidance is available for planning SCM.

The impact to the NRC would be the costs associated with preparing and issuing the revised regulatory guide. The impact to the public would be the voluntary costs associated with reviewing and providing comments to the NRC during the public comment period. The value to the NRC and its applicants would be the benefits associated with enhanced efficiency and effectiveness in using a common guidance document as the technical basis for license applications and other interactions between the NRC and its regulated entities.

Pre-Decisional

Conclusions

Based on this regulatory analysis, the NRC staff recommends revision of Regulatory Guide 1.169. The staff concludes that the proposed action will enhance reactor safety by providing clear guidance for planning SCM. The revision of this guide could also reduce regulatory uncertainty and thereby minimize the costs for the industry, especially with regard to applications for standard plant design certifications and combined licenses.

Pre-Decisional

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

8. Code of Federal Regulations (CFR), *Title 10, Energy,* Part 50, "Domestic Licensing of Production and Utilization Facilities," U.S. NRC, Washington, DC.

9. American National Standards Institute, Institute of Electrical and Electronic Engineers (ANSI/IEEE) Std. 1042-1987, "IEEE Guide to Software Configuration Management," ANSI/IEEE, Piscataway, NJ, 1987.[2]

10. CFR, *Title 10, Energy*, Part 73, "Physical Protection of Plants and Materials," U.S. NRC, Washington, DC.

11. NRC, Regulatory Guide 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," U.S. NRC, Washington, DC.

12. 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.

Pre-Decisional

---

[1] Publicly available NRC 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 American National Standards Institute (ANSI) standards may be purchased from ANSI, 1819 L Street, NW, Washington, DC 20036, on their Web site at http://webstore.ansi.org/; telephone (202) 293-8020; fax (202) 293-9287; or e-mail storemanager@ansi.org.

13. 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.

14. 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.

15. NRC, Regulatory Guide 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," U.S. Nuclear Regulatory Commission, Washington, DC.

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

17. NRC, NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," March 2007.

Pre-Decisional