REGULATORY ANALYSIS

DRAFT REGULATORY GUIDE DG-1210

Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants

(Proposed Revision 1 of Regulatory Guide 1.173, 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 for achieving the intent of NRC's regulations. Many industries where computers and software are replacing traditional hardware-only instrumentation and control (I&C) designs are facing this problem. To this extent, the nuclear industry is not very different from any industry associated with high-consequence hazards. While 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 give rise to concerns about design verification and quality assurance; the increase in 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" (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" (Ref. 2).

Subsequently, the NRC sponsored studies that resulted in 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," 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. While it is possible to simply list the criteria covered, the problem still remains of reaching a common understanding between the NRC staff and industry practitioners regarding what constitutes acceptable software engineering practices for safety systems. An agreed-upon collection of standards, established practices, and engineering techniques for software engineering methods is needed 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.

A disciplined, planned method for creating and following a software life cycle is fundamental to the assurance of software quality, as evidenced by the large body of literature on the subject. Correct method development depends upon careful planning and execution. For systems and components under its purview, Section III, "Design Control," of Appendix B to 10 CFR Part 50 requires that applicable regulatory requirements and the design basis be correctly translated into specifications in design

documents. For software systems, a software life cycle should be planned and executed. A common understanding between the staff and applicants of an acceptable method for accomplishing the development of a software life cycle will improve software system development and modification and benefit staff safety reviews significantly.

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 1.173.
- Update Regulatory Guide 1.173.

Alternative 1: Do Not Revise Regulatory Guide 1.173

Under this alternative, the NRC would not revise this guidance, and the original version of this regulatory guide would continue to be used. This alternative is considered the baseline or "no action" alternative and, as such, involves no value/impact considerations.

The impact associated with not revising the regulatory guide to endorse IEEE Std 1074-2006, "IEEE Standard for Developing a Software Project Life Cycle Process" (Ref. 8) is that the NRC, its licensees, and applicants may interpret differently the level of detail, types, and amount of software development lifecycle controls needed for safety system software. The current version of the regulatory guide endorses IEEE Std 1074-1995 which does not provide the same quantity of information on software development processes as contained in the 2006 revision. Continuation of the current regulatory guide does not reduce the regulatory uncertainties associated with the inputs, development, verification or control processes, and outputs currently accepted as necessary for a well-coordinate software development process. 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 other software engineering regulatory guides (e.g., RG 1.168 "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" [Ref. 9]; RG 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety

Systems of Nuclear Power Plants, [Ref. 10]; RG 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" [Ref. 11]; RG 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" [Ref. 12]; and RG 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" [Ref. 13]) have been updated or are being updated in parallel with this revision.

Alternative 2: Update the Regulatory Guide 1.173

Under this alternative, the NRC would update Regulatory Guide 1.173, taking into consideration the enhanced consensus practices for developing software life cycle processes for digital computer software used in safety systems of nuclear power plants embodied in the current version of IEEE Std 1074-2006.

Significant changes to the regulatory requirements and guidance associated with Regulatory Guide 1.173 have been made. Revising the guide to account for these changes would clarify the guide's position within the regulatory framework and would maintain the set of software engineering regulatory guides as a self-consistent whole.

Effectively, updating Regulatory Guide 1.173 to endorse the new version of the IEEE standard will (1) simplify the staff's review process and enable licensees/applicants to develop a unified, coherent means of meeting the requirements of 10 CFR Part 50 and (2) reduce regulatory uncertainty and, thereby, help to minimize the costs associated with the implementation of this guide.

The costs to the NRC would be the one-time cost of issuing the revised regulatory guide (which is expected to be relatively small) and applicants would incur little or no cost.

Conclusions

There are a number of potential benefits associated with the use of digital I&C safety systems in nuclear power plants. Implementations of these systems should be consistent with the Commission's regulations. Two approaches to providing additional guidance for software were examined. Endorsing the revised software engineering standard has good value with minimal impact and addresses the stated problem. Note that this endorsement presents no new regulatory requirement; it defines acceptable approaches for meeting existing requirements.

REFERENCES[1]

1. U.S. Nuclear Regulatory Commission (NRC), SECY 91-292, "Digital Computer Systems for Advanced Light Water Reactors," 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," NRC, Washington, DC, April 2, 1993. (ADAMS Accession Number ML003708021)
3. NRC, NUREG/CR-6101, "Software Reliability and Safety in Nuclear Reactor Protection Systems," NRC, Washington, DC, November 1993. (ADAMS Accession No. 072750055)
4. NRC, NUREG/CR-6113, "Class 1E Digital Systems Studies," NRC, Washington, DC, October 1993. (ADAMS Accession No. ML062510120)
5. NRC, NUREG/CR-6263, "High Integrity Software for Nuclear Power Plants: Candidate Guidelines, Technical Basis and Research Needs," NRC, Washington, DC, June 1995. (ADAMS Accession No. ML063470590, ML063470593, and ML063600344)
6. NRC, NUREG/CR-6293, "Verification and Validation Guidelines for High Integrity Systems," NRC, Washington, DC, issued March 1995. (ADAMS Accession No. ML070310166 and ML070320556)
7. NRC, NUREG/CR-6294, "Design Factors for Safety-Critical Software," NRC, Washington, DC, December 1994.
8. Institute of Electrical and Electronic Engineers (IEEE), Std 1074-2006, "IEEE Standard for Developing a Software Project Life Cycle Process" IEEE, Piscataway, NJ, 2006.[2]
9. NRC, Regulatory Guide 1.168, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," NRC, Washington, DC
10. NRC, Regulatory Guide 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," NRC, Washington, DC
11. NRC, Regulatory Guide 1.170 "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," NRC, Washington, DC
12. NRC, Regulatory Guide 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," NRC, Washington, DC
13. NRC, Regulatory Guide 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," NRC, Washington, DC.

[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 are also available for inspection or copying for a fee from the NRC's Public Document Room (PDR) at 11555 Rockville Pike, Rockville, MD; the mailing address is US NRC 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, PO Box 1331, Piscataway, NJ 08855 or through the IEEE's public Web site at http://www.ieee.org/publications_standards/index.html.