# REGULATORY ANALYSIS

## DRAFT REGULATORY GUIDE DG-1267
## Verification, Validation, Reviews, and Audits for Digital Computer Software used in Safety Systems of Nuclear Power Plants

(Proposed Revision 2 of Regulatory Guide 1.168, dated February 2004)

### 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 for achieving the intent of NRC regulations. Many industries where computers and software are replacing traditional hardware-only 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 raise 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," 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 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 verification and validation (V&V) is fundamental to the assurance of software quality, as evidenced by the large body of literature on the subject. An effective V&V program depends on careful planning and execution and this, in turn, depends partially on appropriate documentation. For systems and components under its purview, Appendix B to 10 CFR Part 50 requires design control, including the use of written design control procedures, design reviews and testing, and documentation of results, as well as the maintenance of sufficient records to furnish evidence of activities affecting quality. The importance of software V&V in the development of safety-related software is stressed in the studies cited above. NUREG/CR-6101, in its description of activities and related documents necessary for the production of reliable software, addresses software V&V in all software life cycle phases. A common understanding between the staff and applicants of an acceptable method for accomplishing software V&V will benefit the safety review process significantly. The NRC developed this regulatory guide to ensure a

common understanding between the staff and applicants of an acceptable method for providing software V&V, reviews, and audits.

Revisions of industry standards endorsed in this guide have captured subsequent experience with many related aspects of software quality assurance. Consequently, retaining Revision 1 of this guide without updating the endorsement of these revised standards would not reflect current best practices. In addition, the regulatory framework described in Revision 1 of the guide does not include recent additions to NRC regulations that apply to new plant licensing.

Therefore, revision of this regulatory guidance is necessary to address the most recent IEEE standards on providing software V&V, reviews, and audits for safety systems 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 1.168.
- Revise Regulatory Guide 1.168.

<u>Alternative 1: Do Not Revise Regulatory Guide 1.168</u>

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 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. 1012-2004 and IEEE Std. 1028-2008 is that the NRC and its licensees and applicants may interpret differently the types and amount of proper activities necessary to plan software V&V, reviews, and audits. Retaining the current version of the regulatory guide does not reduce regulatory uncertainties with respect to software V&V, reviews, and audits as the NRC staff and licensees and applicants try to reconcile variations in descriptions of the regulatory framework, as well as the usage of multiple versions of industry standards. This is partly due to the current version of regulatory guide does not address numerous changes in the regulatory environment:

10 CFR Part 73 has been amended to add new security requirements including cyber security requirements (10 CFR 73.54).

The other software engineering regulatory guides [RG 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Ref. 8), RG 1.170

"Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Ref. 9), RG 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Ref. 10), RG 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Ref. 11), and RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Ref. 12)] have been updated or are being updated in parallel with this revision.

Alternative 2: Revise Regulatory Guide 1.168

Under this alternative, the NRC would revise Regulatory Guide 1.168, taking into consideration the enhanced consensus practices for planning software V&V, reviews, and audits as embodied in the current version of IEEE Std 1012-2004 and IEEE Std 1028-2008. The review guidance contained in Chapter 7 of NUREG-0800 also addresses implementation of those processes.

Revising Regulatory Guide 1.168 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 software V&V, reviews, and audits.

The impact to the NRC would be the costs associated with preparing and issuing the regulatory guide revision. 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 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.

**Conclusions**

Based on this regulatory analysis, the NRC staff recommends revision of Regulatory Guide 1.168. The staff concludes that the proposed action will enhance reactor safety by providing clear guidance for planning software V&V, reviews, and audits. 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," 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.

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

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

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

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

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

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

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

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

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


[1] Publicly available documents from the U.S. Nuclear Regulatory Commission (NRC) are available electronically through the NRC Library on the NRC's public Web site at http://www.nrc.gov/reading-rm/doc-collections/. The documents can also be viewed on-line for free 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.