UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, DC 20555 - 0001

June 18, 2013

Mr. R.W. Borchardt
Executive Director for Operations
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: DRAFT FINAL REVISIONS OF REGULATORY GUIDES 1.168 THROUGH 1.173, SOFTWARE PROCESSES FOR DIGITAL COMPUTERS IN SAFETY SYSTEMS OF NUCLEAR POWER PLANTS

Dear Mr. Borchardt:

During the 605th meeting of the Advisory Committee on Reactor Safeguards, June 5-7, 2013, we completed our review of the draft final revisions (Rev) of the following Regulatory Guides (RG) for processes for digital computer software used in safety systems of nuclear power plants:

- RG 1.168 Rev 2, Verification, Validation (V&V), Review, and Audits
- RG 1.169 Rev 1, Configuration Management
- RG 1.170 Rev 1, Test Documentation
- RG 1.171 Rev 1, Unit Testing
- RG 1.172 Rev 1, Software Requirements Specifications
- RG 1.173 Rev 1, Developing Software Life-Cycle Processes

Our Digital Instrumentation &Control (DI&C) Systems Subcommittee also reviewed this matter during a meeting on May 21, 2013. During these reviews, we had the benefit of discussions with representatives of the NRC staff and comments from industry representatives. We also had the benefit of the documents referenced.

RECOMMENDATIONS

1. Draft final revisions to RG 1.168 Rev 2, Verification, Validation, Review, and Audits; RG 1.169 Rev 1, Configuration Management; RG 1.170 Rev 1, Test Documentation; RG 1.171 Rev 1, Unit Testing; RG 1.172 Rev 1, Software Requirements Specifications; and RG 1.173 Rev 1, Developing Software Life-Cycle Processes should be issued.

2. The staff should expedite the development of consistent regulatory guidance for enhanced design, development, operation, and maintenance of digital hardware and software which controls non-safety-related equipment that is “important to safety.”

BACKGROUND

Regulatory Guides 1.168 through 1.173 were first issued in September 1997 in order to provide regulatory guidance for the development of processes for digital computer software used in safety systems of nuclear power plants. These RGs were based on and endorsed Institute of Electrical and Electronics Engineers (IEEE) standards that were utilized by industry prior to 1997. With the exception of RG 1.168, which had a revision in February 2004 to IEEE standards issued in 1997 and 1998, none of these RGs have had any updates.

The impetus for the RG revisions was to review and evaluate updated versions of the IEEE standards originally endorsed by the guides so that these more current versions could be endorsed. In addition, lessons learned over the last decade in the application of the RGs have been incorporated to clarify positions and remove ambiguities.

DISCUSSION

The updated IEEE standards in each of the RGs are as follows.

- RG 1.168: IEEE-1012 (1998 to 2004) and IEEE 1028 (1997 to 2008)
- RG 1.169: IEEE-828 (1990 to 2005)
- RG 1.170: IEEE-829 (1983 to 2008)
- RG 1.171: IEEE-1008 (1987 reaffirmed in 2002)
- RG 1.172: IEEE-830 (1993 to 1998)
- RG 1.173: IEEE-1074 (1995 to 2006)

All of the revised RGs follow the endorsed IEEE standards directly and identify exceptions where appropriate. Where Annexes are included in the IEEE standards, the RGs clearly identify which are endorsed and which are not. A summary of significant changes and exceptions follows:

1. RG 1.168 Rev. 2, Verification, Validation, Review, and Audits - There were minimum regulatory changes to this RG based on the revised IEEE standards. There were two exceptions as noted below.

    a. IEEE Standard 1012, Annex C defined a new form of independence for V&V organizations called “conditional independence” which would allow less rigorous independence of the V&V technical, managerial, and financial organizations from the software development organization. Regulatory Position 8 takes exception to this new form of independence and refers to Branch Technical Position 7-14 for guidance on the independence of software reviews.

    b. IEEE Standard 1012, Annex F includes an organizational structure diagram Figure F.1, “Relationship of V&V to other project responsibilities.” Regulatory Position 3 takes exception to subordinate relationships outside of the major relationships.

2. RG 1.169 Rev. 1, Configuration Management - There were several additions to this RG that complement the supporting IEEE standards associated changes. The major ones are noted below. There were no exceptions.

    a. The RG incorporated guidance for acceptance of commercial grade software in Regulatory Position 7, referencing previously endorsed EPRI Topical Report-106439 issued in 1996.

    b. The RG incorporated a new Regulatory Position 12 on release management and delivery to include sufficient control for correction of faults.

3. RG 1.170 Rev. 1, Test Documentation - There are major additions to the RG based on the significantly revised IEEE standard. The revised standard outlines integrity levels, documentation strategies, and process directions. It builds a Master Test Plan that improves planning and reporting, improves focus for multiple levels of software testing, and completes the testing loop with formal documentation of anomalies. There were two exceptions as noted below.

    a. IEEE Standard 829 allows a software integrity level less than 4 for safety system software based on analysis methods defined in Annex B, Table B.3, Risk Assessment Scheme. The RG adds a new Regulatory Position 6, “Integrity Levels,” that states only an integrity level 4 should be assigned for nuclear power plant safety systems.

    b. IEEE Standard 829 does not require repeat test information if the information is managed with an automated test tool. Since there are cases where electronic validation methods with repetitive information are needed to form a safety conclusion, the RG adds a new Regulatory Position 8, “Test Tool Documentation,” that takes exception to this allowance.

4. RG 1.171 Rev. 1, Unit Testing - There were no substantial changes to this RG. There were no exceptions.

5. RG 1.172 Rev. 1, Software Requirements Specifications - There were minor changes to this RG to provide emphasis on clear specifications and a new overview on secure analysis. There were no exceptions.

6. RG 1.173 Rev. 1, Developing Software Life-Cycle Processes - While there were numerous revisions to the endorsed IEEE standard, they consisted primarily of rearrangement of clauses and some improvements to activities in Annex A. The significant RG changes and one exception are noted below.

a. New Regulatory Position 1.d, “Secure Analysis,” was added which takes exception to IEEE Standard 1074 directions for security assurance level in Section A.1.1.5, "Determine Security Objectives (Required)." The position refers to RG 1.152 for secure software development guidance and to RG 5.71 for cyber security guidance.

b. New Regulatory Position 4.d, “System Transitions,” states that all changes to safety systems must be evaluated using the criteria of 10 CFR 50.59 rather than just those that are a complete replacement with new or revised systems as allowed in IEEE Standard 1074, Section 4.1.2.3, “Plan System Transition.”

The revised RGs should be issued.

A footnote in each of these RGs states:

The term "safety systems" is synonymous with "safety-related systems." The scope of the GDC includes structures, systems, and components "important to safety." However, the scope of this regulatory guide is limited to "safety systems," which are a subset of "systems important to safety."

The current regulatory framework for operating reactors licensed under 10 CFR Part 50 and for new plants licensed under 10 CFR Part 52 contains provisions for enhanced design, quality, reliability, and regulatory oversight for non-safety-related structures, systems, and components (SSCs) that are “important to safety.” Examples of these provisions are addressed in 10 CFR 50.65 (the maintenance rule), 10 CFR 50.69 (risk-informed treatment of SSCs), and RG 1.206 (enhanced controls for non-safety-related SSCs under the Regulatory Treatment of Non-Safety Systems and Reliability Assurance Programs). These enhanced programs generally apply criteria that are less stringent than the requirements for safety-related SSCs, but are more restrictive than the criteria for other non-safety-related SSCs.

Operating plants are upgrading their aging analog equipment to digital instrumentation, control, and protection systems. All new plant designs rely extensively on digital systems. Non-safety-related digital hardware and software systems actuate, control, and monitor the operation of associated non-safety-related pumps, valves, etc. which are “important to safety.” These digital systems are explicitly excluded from the scope of the regulatory guides discussed in this report. That treatment is incongruous with consistent regulatory oversight of SSCs that are “important to safety.”

The IEEE standards that are referenced in these RGs define four levels of integrity for software, depending on the importance of the controlled functions. The staff should expedite the development of consistent regulatory guidance for enhanced design, development, operation, and maintenance of digital hardware and software which controls non-safety-related equipment that is "important to safety."

We commend the staff for their efforts in completing this extensive revision to six related guides for digital computer software for safety systems in nuclear power plants.

Additional comments by ACRS Members D.A. Powers, D.C. Bley, J.W. Stetkar, M. Ryan, J.L. Rempe, C.H. Brown Jr., J.S. Armijo, and S.P. Schultz are presented below.

Sincerely,

/RA/

J. Sam Armijo
Chairman

Additional Comments from D.A. Powers, D.C. Bley, J.W. Stetkar, M. Ryan, J.L. Rempe, C.H. Brown, Jr., J.S. Armijo and S.P. Schultz.

Classification of structures, systems and components as 'safety related' or 'non-safety-related' is an anachronism. This type of classification is based on traditional considerations of design basis accidents and their associated analytical requirements and assumptions. In important cases, this legacy classification can be displaced by a more meaningful classification based on probabilistic risk assessment. It is important that systems found to be important to plant safety by the systematic and scrutable use of probabilistic risk assessment receive appropriately high levels of licensee and regulatory attention whether these systems are considered to be 'safety related' or not. Software and digital hardware found to be important for plant safety should be subjected to stringent quality requirements. This certainly should be the case for software. Software is vulnerable not only to human error during its development, use and updating, but also to malicious attack by skilled and determined individuals and organizations. Consequently, software that controls systems demonstrated to be important to plant safety could be required to meet the same stringent quality requirements as do software controlling 'safety related' systems. This would be a natural starting point that could be adapted as experience yields an understanding of what parts of the prescriptive approach can be eliminated, made less stringent, or replaced with more efficient and effective approaches. The quality requirements imposed on systems found to be important to plant safety could, of course, be tailored based on the insights derived from risk analyses.

It will be useful to both the agency and its licensees to make greater use of probabilistic risk assessment for the safety categorization of structures, systems and components. This may be especially true for the review of modern reactors and advanced reactors. Even for existing nuclear power plants, categorization based on probabilistic risk assessment provides additional insights about how systems should be most appropriately protected and maintained to provide

assurance that they will be available during events when they are needed. 10 CFR 50.69 and its associated guidance provide a regulatory basis for applying this more structured process. Current guidance such as that provided in the Regulatory Guides discussed in this report may merit refinement to resolve quandaries about the appropriate quality treatment of 'non-safety-related' items found to be important to plant safety by probabilistic risk assessment. The availability of such guidance could encourage plants to implement 10 CFR 50.69 which provides a better focus for the efforts NRC and licensees make to assure that structures, systems and components have appropriate quality for their function.

REFERENCES

1. Package to E. Hackett, ACRS from M. Case, RES on Revision 2 of RG 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software used in Safety Systems of Nuclear Power Plants," issued for public comment as DG-1267, August 23, 2012 (ML12236A132).

2. Package to E. Hackett, ACRS from M. Case, RES on Revision 1 of RG 1.169, "Configuration Management Plans for Digital Computer Software used in Safety Systems of Nuclear Power Plants," issued for public comment as DG-1206, December 19, 2012 (ML12354A524).

3. Package to E. Hackett, ACRS from M. Case, RES on Revision 1 of RG 1.170, "Test Documentation for Digital Computer Software used in Safety Systems of Nuclear Power Plants," issued for public comment as DG-1207, December 19, 2012 (ML12354A531).

4. Package to E. Hackett, ACRS from M. Case, RES on Revision 1 of RG 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," issued for public comment as DG-1208, December 19, 2012 (ML12354A534).

5. Package to E. Hackett, ACRS from M. Case, RES on Revision 1 of RG 1.172, "Software Requirements Specifications for Digital Computer Software used in Safety Systems of Nuclear Power Plants," issued for public comment as DG-1209, December 19, 2012 (ML12354A538).

6. Package to E. Hackett, ACRS from M. Case, RES on Revision 1 of RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants," issued for public comment as DG-1210, January 8, 2013 (ML13008A338).

7. Regulatory Guide 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," U.S. NRC, Washington, DC, Rev. 3, July 31, 2011 (ML102870022).

8. Regulatory Guide RG 5.71, "Cyber Security Programs for Nuclear Facilities," Rev 0, January 31, 2009 (ML090340159).

9. Regulatory Guide, 1.206, "Combined Applications for Nuclear Power Plants," June 20, 2007 (ML070720184).

10. IEEE Std. 7-4.3.2-2003, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,” IEEE, NJ, 2003.

11. Electric Power Research Institute (EPRI) TR-106439, “Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications,” EPRI, Palo Alto, CA, 1996.

12. Letter from Matthews, D. B., Chief, Generic Issues and Environmental Projects Branch, Division of Reactor Program Management, NRC, to Torok, R.C., Project Manager, Nuclear Power Group, EPRI, titled “Review of EPRI topical report TR-106439, ‘Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications’ (TAC No. M94127)” dated July 17, 1997 (ML092190664).

10. IEEE Std. 7-4.3.2-2003, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,” IEEE, NJ, 2003.

11. Electric Power Research Institute (EPRI) TR-106439, “Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications,” EPRI, Palo Alto, CA, 1996.

12. Letter from Matthews, D. B., Chief, Generic Issues and Environmental Projects Branch, Division of Reactor Program Management, NRC, to Torok, R.C., Project Manager, Nuclear Power Group, EPRI, titled “Review of EPRI topical report TR-106439, ‘Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications’ (TAC No. M94127)” dated July 17, 1997 (ML092190664).

Accession No: ML13161A243 **Publicly Available Y** **Sensitive N**
Viewing Rights: ☒ NRC Users or ☐ ACRS Only or ☐ See Restricted distribution

OFFICE	ACRS	SUNSI Review	ACRS	ACRS	ACRS
NAME	CAntonescu	CAntonescu	CSantos	EMHackett	EMH for JSA
DATE	6/18/13	6/18/13	6/18/13	6/18/13	6/18/13

OFFICIAL RECORD COPY