ROB received
3/15/05

March 14, 2005

1107 Live Oak Circle
Knoxville, TN 37932

12/16/04
69FR73359
(14)

U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

To Whom It May Concern:

Subject: Comments on DG-1130

Draft Guide 1130 (DG-1130), "Criteria For Use Of Computers In Safety Systems of Nuclear Power Plants," provides U.S. Nuclear Regulatory Commission (NRC) staff endorsement of the 2003 revision of Institute of Electrical and Electronics Engineers (IEEE) standard 7-4.3.2, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations." This draft guide is a revision of existing regulatory Guide (RG) 1.152, Revision 1, which endorsed IEEE 7-4.3.2-1993 with one exception. That exception involves a clause (§5.15) in the standard that addressed reliability goals. The exception was that sole reliance on quantitative reliability goals was unacceptable.

DG-1130 states that conformance with the requirements of IEEE 7-4.3.2-2003 is acceptable, with one exception, for satisfying the Commission's regulations with respect to high functional reliability and design requirements for computer-based safety systems. The exception is taken to a clause (§5.6(a)) in the standard regarding the use of barriers as a means of ensuring independence between safety and nonsafety functions implemented on the same computer. Another clause (§5.6(b)) within the standard is identified as being an acceptable alternative. Additionally, DG-1130 provides a regulatory position containing explicit guidance related to security to supplement the criteria provided in the standard.

The regulatory analysis accompanying the draft guide provides a brief overview of significant changes embodied in the revised standard. However, there is no discussion of the potential impact of these changes on existing practices or staff positions nor is there reference to any document that provides the technical basis to support the endorsement of this standard. Likewise, there is no discussion of the resolution of the standing exception to the 1993 version of the standard that was taken in the existing regulatory guide. The absence of a documented technical basis suggests that perhaps a more detailed assessment of the changes in the standard and their regulatory significance might be warranted.

SISP Review Complete

Template = ADM-013

E-RFDS=ADM-03

Cell = S. Aggarwal (SKA)

By comparing 1993 and 2003 versions of the standard, it is clear that a significant change in the guidance on equipment qualification was introduced. The 1993 version of IEEE 7-4.3.2 states the following in section 5.4, entitled "Equipment qualification."

> In addition to the requirements of IEEE Std 603-1991, the following requirement is necessary in order to meet the equipment qualification criterion.
>
> Equipment qualification testing shall be performed with the computer functioning with software and diagnostics that are representative of those used in actual operation. All portions of the computer necessary to accomplish the safety function, or those portions whose operation or failure could impair the safety function, shall be exercised during testing. This includes, as appropriate, exercising and monitoring the memory, the CPU, inputs and outputs, display functions, diagnostics, associated components, communication paths, and interfaces. Testing shall demonstrate that the design basis performance requirements have been met.

Equipment qualification has a very specific meaning and the IEEE definition can be found in IEEE standard 323, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations." That definition, as expressed in the 2003 version of the standard, is as follows.

> 3.10 equipment qualification: The generation and maintenance of evidence to ensure that equipment will operate on demand to meet system performance requirements during normal and abnormal service conditions and postulated design basis events.
>
> NOTE – Equipment qualification includes environmental and seismic qualification.

The 2003 version of IEEE 7.4.3.2 alters the focus of the equipment qualification section by changing the wording to invoke the concept of computer system qualification testing, as something distinct from equipment qualification. Additionally, additional criteria regarding the qualification of existing commercial computers is added. The criteria on equipment qualification that is comparable to that given in the 1993 version of the standard is as follows.

> 5.4. Equipment qualification.
>
> In addition to the equipment qualification criteria provided by IEEE Std 603-1998, the requirements listed in 5.4.1 and 5.4.2 are necessary to qualify digital computers for use in safety systems.

5.4.1 Computer system testing

Computer system qualification testing (see 3.1.36) shall be performed with the computer functioning with software and diagnostics that are representative of those used in actual operation. All portions of the computer necessary to accomplish safety functions, or those portions whose operation or failure could impair safety functions, shall be exercised during testing. This includes, as appropriate, exercising and monitoring the memory, the CPU, inputs and outputs, display functions, diagnostics, associated components, communication paths, and interfaces. Testing shall demonstrate that the performance requirements related to safety functions have been met.

The referenced definition within IEEE 7-4.3.2-2003, along with additional definitions of associated terms, is as follows.

3.1.36 qualification testing: Testing performed to demonstrate to the acquirer that the software item or system meets its specified requirements.

3.1.46 system testing: Testing conducted on a complete, integrated system to evaluate the system's compliance with its specified requirements.

3.1.47 testing: (1) The process of operating a system or component under specified conditions, observing or recording the results, and making an evaluation of some aspect of the system or component. (2) The process of analyzing a software item to detect the difference between existing and required conditions (that is, bugs) and to evaluate the features of the software items.

3.1.1 acceptance testing: (1) Formal testing conducted to determine whether or not a system satisfies its acceptance criteria and to enable the customer to determine whether or not to accept the system. See also: qualification testing, system testing. (2) Formal testing conducted to enable a user, customer, or other authorized entity to determine whether to accept a system or component.

It does not appear that the testing required in the 2003 version of the standard is equivalent to that required in the 1993 version. Certainly, equipment qualification testing, as defined by the IEEE, provides for a thorough investigation of the environmental susceptibility of the equipment under test as it is subjected to the environmental extremes of its anticipated service condition. There is no indication that such testing is incorporated in the new, more broadly defined computer system qualification testing. In fact, given the wording of the qualification testing definition along with the associated definitions of testing, it appears that the 2003 version of the standard has relaxed the scope of equipment qualification testing to practices that are more equivalent to acceptance testing rather than the traditional environmental

qualification testing. This rather significant change in the criteria embodied within the standard is not acknowledged in the summary of changes given by the regulatory analysis of DG-1130.

Another issue of concern arises from the new section 5.4.2 on qualification of existing commercial computers. This additional clause appears to permit omission of equipment qualification testing without a requirement that the justification be established and documented. The main criteria given in the standard are as follows.

> 5.4.2 Qualification of existing commercial computers
>
> NOTE—See Annex C for more information about commercial grade item dedication.
>
> The qualification process shall be accomplished by evaluating the hardware and software design using the criteria of this standard. Acceptance shall be based upon evidence that the digital system or component, including hardware, software, firmware and interfaces, can perform its required functions. The acceptance and its basis shall be documented and maintained with the qualification documentation.
>
> In those cases in which traditional qualification processes cannot be applied, an alternative approach to verify a component is acceptable for use in a safety-related application is commercial grade dedication. The objective of commercial grade dedication is to verify that the item being dedicated is equivalent in quality to equipment developed under a 10 CFR 50 Appendix B program [B15].
>
> The dedication process for the computer shall entail identification of the physical, performance, and development process requirements necessary to provide adequate confidence that the proposed digital system or component can achieve the safety function. The dedication process shall apply to the computer hardware, software, and firmware that are required to accomplish the safety function. The dedication process for software and firmware shall, whenever possible, include an evaluation of the design process. There may be some instances in which a design process cannot be evaluated as part of the dedication process. For example, the organization performing the evaluation may not have access to the design process information for a microprocessor chip to be used in the safety system. In this case, it would not be possible to perform an evaluation to support the dedication. Because the dedication process involves all aspects of life cycle processes and manufacturing quality, commercial grade item dedication should be limited to items that are relatively simple in function relative to their intended use.

The qualification processes identified in this section extend well beyond the "traditional qualification processes" that are established for equipment qualification in IEEE 323. While it is acknowledged that design qualification is an important element of ensuring that computer-based safety systems are appropriate for the safety application, the inclusion of these broader processes under the heading of equipment qualification has the potential to obscure the need for traditional equipment qualification testing. As a result, it is conceivable that a user of this guidance could decide that equipment qualification (i.e., testing under environmental extremes of the expected service condition as is required in IEEE 7-4.3.2-1993) cannot be applied for a commercial computer. Since there is no requirement for deviation from "traditional qualification processes' to be explicitly justified with a technical basis and there is no guidance on how to establish such justification, the simple determination that those processes are too expensive could be used. Existing guidance for commercial dedication (e.g., EPRI 107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants") includes explicit guidance for environmental qualification testing. It is difficult to imagine safety system implementations using commercial computers that would result in a technical impediment to testing the equipment under exposure to the environmental extremes that are associated with its expected service conditions. It should be made clear that the requirement for testing, which exists without exception in IEEE 7-4.3.2-1993, is maintained in the endorsement of the revised standard even for commercial computer qualification.

The bottom line to consider is that the current NRC staff position, as expressed in RG 1.152, Rev. 1, endorses the requirement for equipment qualification testing of computer-based safety systems in which the computer is functioning with representative operational software and diagnostics. The regulatory position expressed in DG-1130 is silent on the differences in qualification criteria between the two versions of the standard and, thus, appears to result in a relaxation of the existing regulatory position without providing any technical justification for doing so.

The specific comments that arise from the above assessment are the following.

1) What is the justification for accepting the change in position regarding equipment qualification testing? Either the technical evidence that supports relaxation of the existing regulatory position needs to be documented and identified or an exception needs to be taken to reaffirm the current position.

2) Why is a requirement to technically justify any omission of traditional equipment qualification processes not included to clarify the application of the criteria for qualifying existing commercial computers? As the guidance now stands, there does not appear to be any threshold established for when deviations from nuclear quality assurance and equipment qualification practices are acceptable. There should be a clarifying exception taken to this clause (§5.4.2).

3) Why was no explanation given regarding the resolution of the exception taken to IEEE 7-4.3.2-1993? A review of the wording in section 5.15 of each version of the standard reveals that there was only a modest revision, with the most notable change being the elimination of the adjectives "qualitative or quantitative," which modify the phrase "reliability goals."

There is considerable value in the U.S.NRC maintaining awareness of evolving consensus standards and endorsing the latest versions of those standards as warranted. However, a critical assessment of the new or modified clauses in revised standards is essential to ensure consistency with well-established positions. It does not appear that this standard received such an assessment or at least the findings of that assessment are not well documented. It is strongly recommended that DG-1130 be modified to account for the issues identified in this comment submission.

Thank you,

Richard T. Wood