MPR ASSOCIATES INC.
ENGINEERS

66FR51479
10/9/01
(4)

December 14, 2001

Ms. C. E. Antonescu
Rules and Directives Branch
Office of Administration, U. S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Subject: Comments on NRC Draft Regulatory Guide DG-1077, "Guidelines for Environmental Qualification of Microprocessor-Based Equipment Important to Safety in Nuclear Power Plants"

Dear Ms. Antonescu:

Below please find comments from MPR Associates, Inc. on the subject draft regulatory guide.

- The draft guide states in the Discussion section (page 3, paragraph 4) that for the purposes of this guide, "qualification" is a verification... under the most limiting environmental stresses that can result from design basis accidents. There are a number of areas in nuclear plants whose environment does not change with design basis accidents. However, the location categories (A, B, and C) do not limit the applicability of the guide to those areas with environmental stresses that can result from design basis accidents. The draft guide should redefine the categories to be consistent with the Discussion section.

- Subparagraph 3 of Section C, Regulatory Position, states that IEEE 323 requires a qualified life for microprocessor-based equipment in a Category A environment. IEEE 323 does not use such terminology. The Guide should be revised. IEEE 323 is consistent with the words in the Discussion section of the draft guide, and addresses qualification for "harsh environments" (i.e., environmental stresses that can result from design basis accidents).

- The existing Harsh and Mild equipment qualification categories do not map into the three newly provided categories. The draft guide should define a method that utilities can use to comply with the new guidance, short of a complete re-evaluation of all currently qualified equipment and re-mapping the existing nuclear plants.

Template = ADM-013

E-RIDS = ADM-03
Add = A. Berasek (AF-B)

320 KING STREET ALEXANDRIA, VA 22314-3230 703-519-0200 FAX: 703-519-0224 http:\\www.mpr.com

C. Antonescu (CEA1)

- There is no basis provided for the use of 400 Rads or 10,000 Rads for equipment qualification for Categories B and C.

- We note that experience shows that MOS semiconductor structures start failing at around 1000 Rads integrated gamma dose to the silicon. This failure mechanism fits well with the current definition used by the nuclear industry for a mild environment, which yields a 40-year exposure of about 1000 Rads. We believe that obsolescence will continue to force digital component replacements about every 15 to 20 years, which invalidates any requirement for a 40-year qualified life.

- Modern analog devices also are built from MOS technologies, and are subject to the same radiation-induced failure mechanisms. However, DG-1077 is applicable only to digital devices. The USNRC should provide consistent regulatory guidnace for the use of MOS technology, whether in digital or analog designs.

- DG-1077 provides several interesting observations about water damage. We note that most of the issues with water damage result from water falling from floors above or pipe breaks above the equipment. Guidance should be provided for water resistance on cabinet tops and ventilation slots in cabinet tops, sides, and doors.

- In the definitions for Category B and C devices, we note several inconsistencies and missing definitions, which should be resolved:

  - The RG defines two different conditions for temperature limits for qualification. The RG fails to define where these temperatures apply, e.g. outside the cabinets, at the top or bottom inside the cabinet, at the board, within the semiconductors, etc.

  - The RG defines an expected total integrated gamma dose for normal conditions; however, no definition is provided for accident or abnormal conditions.

  - The RG defines normal conditions as having temperatures less than 100 °F and relative humidity less than 80%. These are not consistent with many nuclear facilities, where normal conditions are defined as 120 °F and 95% relative humidity, non-condensing. Further, there appears to be no basis for forcing modifications in safety-related HVAC systems to support this more restrictive definition of normal conditions.

  - For Category B, the RG defines abnormal and accident conditions the same as normal conditions. As noted above, many nuclear facilities cannot maintain the "normal conditions" defined in the RG during accident and abnormal conditions. Rather, the conditions are limited to 120 °F and 95% relative humidity, non-condensing. There appears to be no basis for forcing modifications in safety-related HVAC systems to support these tighter conditions.

  - For Category C, the RG defines abnormal and accident condition temperatures as being limited to less than 90% of the manufacturer's maximum temperature limits and 95%

relative humidity. We are concerned that without precise definition of the location of the measured temperature, the conditions specified may exceed the chip capability. This would be especially true if integrated circuits are installed in tightly sealed enclosures.

- For Category B, the RG defines a total integrated dose of 10,000 Rads to the silicon. Unless the digital devices are implemented in radiation hardened integrated circuits, standard commercial devices will not withstand that level of radiation. In order to assure that the digital devices would survive this exposure level, about an inch of lead or two inches of steel would be required for shielding.

- We conclude that the guidelines provided in this section are applicable and targeted to new designs, built especially for nuclear use. However, we note that with the exception of some specialized analog replacement devices being designed now, no plant licensee is requesting special nuclear-only digital designs. Thus, we question the utility of this section.

- Most (if not all) of the digital devices that are being installed in nuclear plants are commercial-off-the-shelf designs. Most of them do employ solder masks, thus following the guidance provided in this RG. We have not seen many commercial devices with conformal coating. Conformal coating is a technique usually reserved for military equipment, or equipment that is designed to be used in high humidity environments. We are not likely to find conformal coating on most equipment. Most design engineers would also state that conformal coating provides a greater resistance to heat flow, and thus would require lower temperature limits than those provided herein.

- The RG establishes a new and quite rigorous approach to qualification of components. The RG appears to ask us to credit the commercial integrated circuit vendor's integrated circuit testing for commercial dedication of these devices. But, in order to accept this credit, the licensee will need to make use of currently existing guidance for commercial grade dedication. The industry and the NRC use EPRI NP-5652, "Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications," for means and methods for acceptance of vendor testing, such as the vendor testing that the RG credits. However, application of EPRI NP-5652 Acceptance Method 2, Commercial Grade Survey of Supplier in Conjunction with a Certificate of Conformance, has always required a quality audit by QA certified inspectors. The EPRI report strongly discouraged use of such surveys when components pass through distributors, which is possible for any COTS integrated circuits. The EPRI report then has the utility incorporate the approved vendors into the Approved Vendor List at the accepting utility. Most utilities then require a Certificate of Conformance for the items. COTS equipment and normal commercial manufacturing practices makes achieving these goals unlikely. The DG must establish methods of qualification that the licensees can implement. The following list of questions must be clarified in the RG.

- Does inclusion of this requirement in this DG require the utilities, or some group such as NUPIC or NPIC, to audit all of the integrated circuit manufacturers, place them on their AVL, and continue to audit them forever?

- Does inclusion of this requirement mean that the utilities are expected to open COTS equipment (voiding the warranty), inventory the integrated circuits, return to the equipment vendor and/or manufacturer, find any traceability maintained by the equipment vendor and/or manufacturer, and then start the process of reviewing lot records for each integrated circuit lot from all the vendors used in this device?

- For purposes of this RG, do the devices characterized as "integrated circuits" include integrated resistor and capacitor packages, or did you intend to restrict the term to only packages containing active devices?

- For purposes of this RG, do we, the licensees, need to perform this review function on chips performing analog functions, or should these requirements be limited only to digital devices? Should mixed function devices, such as analog to digital converters and digital potentiometers, be included in this review?

- We question the ability of any utility to assure this traceability and perform the mandated audits on COTS equipment. This activity would have to be performed after the device is received, so there is no chance of implementing Acceptance Method 3, Source Verification, for the integrated circuits.

- We question the need for this activity, based on purchase of qualified devices, which the vendor assures us are built from commercially dedicated devices or assemblies already subjected to an EPRI-5654 compliant process, which the NRC has earlier accepted.

- In general, we question the value of this section, based on the ideas that we are either purchasing equipment from a 10 CFR 50 Appendix B vendor program or commercially dedicated through a 10 CFR 50 Appendix B program. In either case, commercially procured items, including integrated circuits, will have been processed through an EPRI NP-5654 compliant program, or equivalent. We fail to see the value added by repeating this requirement in this RG.

- "First, qualification should begin at the IC manufacturing level... built in quality can be enhanced by ensuring, among other process control methodologies, a minimum of stress tests and a guarantee of correct operation in a specified environment." These tests by the manufacturer "guarantee" nothing; rather, they MINIMIZE the likelihood of failure.

- Clarification is required for the statement "Despite these qualification stress tests at the IC component level, tests documented in NUREG/CR-6406 show that at high relative humidity, digital equipment can fail at temperatures considerably below (the) manufacturer's maximum

operating limit. Thus, (the) manufacturer's ratings alone cannot be relied upon to guarantee reliable operation under abnormal and accident nuclear power plant environments."

- The statement is ambiguous. One reading would assure us that the vendor's specifications can not be believed or trusted, since elevated temperature and humidity testing fails at levels significantly below the manufacturer's specifications. A more benign reading would be that integrated circuits fail no matter what the temperature or humidity. Other interpretations are possible. The DG should be clarified to clearly convey the requirement.

- We question the use of the word "guarantee" since not even the integrated circuit manufacturer will guarantee that their equipment does not fail. In fact, their specifications and ratings are based on the idea that staying within the ratings will maintain the failure rates at their specified levels; in other words, use outside their ratings will increase failure rates. Again, we suggest that the RG be clarified.

- In Section C, Item 10, page 9, the elements mentioned are methods of addressing random failures. We would suggest adding guidance that a visible, easily observed method for annunciating these failures to Operations, Maintenance, or Engineering staff be provided. Many failures have been obvious only when someone queried a user interface, observed a lamp hidden behind closed and locked cabinet doors, or opened the display screen where a small, innocuous message indicated a failure.

- In Section C, Item 10, page 9, in the discussion on diagnostics, generalized guidance was provided that advanced and on-line diagnostics are a good idea. There is a caution provided that overly involved or complex diagnostics are a bad idea, as they may result in additional failure modes or faults. The RG should provide some guidance as to the meanings the NRC applies to "complex" and "involved."

- In Section C, Item 10, page 9, the DG states that "These will minimize the chance for multiple latent failures that are detected only when the equipment is demanded to operate." In risk assessment, one may have a single latent fault that becomes a failure, and multiple latent faults are not required. The RG should be re-worded accordingly. The DG should also contain a definition of the word "latent."

Sincerely,

David Herrell

320 KING STREET ALEXANDRIA, VA 22314-3230 703-519-0200 FAX: 703-519-0224 http:\\www.mpr.com