ADAMS Received 2/11/05

Comments on Draft Regulatory Guide DG-1130

12/16/04
69 FR 75359
(4)

I am an engineer from Taiwan Power Company. Currently, I am working on I&C systems of Lungmen NPP project. Here are some comments on the draft Regulatory Guide:

1. On Page 4, Annex C, "Dedication of Existing Commercial Computers," is not endorsed by the NRC because it provides inadequate guidance. Adequate guidance is available in EPRI TR-106439. However,
   - On Page 3-7 of EPRI-TR-106439, it says "Appendix D of IEEE 7-4.3.2 provides additional guidance on commercial grade item dedication".
   - 7-4.3.2-1993 Annex D "Dedication of existing commercial computers" was updated to more completely address COTS issues and was designated Annex C in 7-4.3.2-2003.
2. On Page 5, Annex D, "Identification and Resolution of Hazards," is not endorsed because it provides inadequate guidance concerning the use of FTA and FMEA and Guidance is provided in Branch Technical Position HICB-14. However,
   - Both FTA and FMEA are not mentioned in BTP HICB-14.
   - The most related topic to Annex D in BTP-14 is software safety analysis. There is only one paragraph in BTP 14 (page BTP HICB-14-26) and the guideline in performing software safety analysis is not clear.
   - IEEE Std 1228-1994 "IEEE Standard for Software Safety Plans" is another important reference to software safety analysis. Comparing Annex D with IEEE 1228-1994 you will find that there is more information available regarding "Identification and resolution of hazards" in computer related software.
3. On Page 6, there is no enough explanation why "Clause 5.6(a) of IEEE Std 7-4.3.2 is not acceptable to NRC".
   - There are ways in implementing the "Barrier" such that technically nonsafety function cannot interference the performance of safety function. For example, in microprocessor, there are different execution modes, namely protection mode and non-protection mode, in microprocessor (e.g., Intel Pentium processor). A program executed in non-protection mode cannot override/interference a program executed in protection mode. There can be a lot of discussion on this issue...
   - Here is what I read from the draft guide: "Safety and nonsafety software may reside on the same computer and use the same computer resources only if nonsafety software is developed using the requirement of safety software." Comparing with the cost of computer hardware and the development of safety software, the easiest way to fulfill this requirement would be "Safety and nonsafety software may not reside on the same computer".
4. On Page 13, "Each postulated common-mode failure should be analyzed using best-estimate methods to address vulnerabilities to common-mode failures."
   - The meaning of this sentence is not clear. What is the intent of NRC in using best-estimate methods?

Chuan-Chung Chen
Department of Nuclear Safety
Taiwan Power Company
Tel: 886-2-23667313(408) 253-7934
E-mail: u808269@taipower.com.tw

SISP Review Complete

E-RIDS=ADM-03
Add=S. Aggarwal (SKA)
P. Harrity (PHI)

Template=ADM-013