Commonwealth Edison Company
1400 Opus Place
Downers Grove, IL 60515-5701

61 FR 46834
9/5/96
JJ Kramer Contact

#4 DS09

October 31, 1996

ComEd

Rules Review and Directives Branch, DOIPS
Office of Administration
U. S. Nuclear Regulatory Commission
Washington, D. C. 20555

SUBJECT: **Commonwealth Edison (ComEd) Comments on Draft Regulatory Guides DG-1054, DG-1055, DG-1055, DG-1056, DG-1057, DG-1058 and DG-1059**

The purpose of this memo is to provide comments to the NRC Staff on draft Regulatory Guides DG-1054, 1055, 1056, 1057, 1058 and 1059. The use of consensus standards is part of an overall approach to meeting the requirements of 10CFR Part 50. Present NRC direction is to define the acceptability of these standards through Regulatory Guides. RegGuide 1.152 endorsed IEEE Std. 7-4.3.2-1993, *Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Plants.* This standard identified a number of IEEE software standards as sources of guidance. The NRC, through these RegGuides, is proposing limited endorsement of these standards. A number of concerns are raised as follows.

DG-1054: Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

This DG will provide an endorsement of IEEE Std. 1012-1986 (V&V) and IEEE Std. 1028-1988 (audits and reviews) with certain stipulations. The stipulations are a source of concern to ComEd.

IEEE Std. 1012 identifies the *software* industry's approach to verification, validation, review and audit activities, not necessarily the nuclear industry's approach. The standard defines a set of "minimum" V&V tasks to be performed for all critical software. DG-1054 correlates critical software with software used in safety systems and requires that these tasks be performed independently of the designer. While the task list may be appropriate for a digital reactor protection system or emergency actuation, it may be much more that what is needed for a safety related control board indicator, radiation monitor, or other similar devices.

The list of minimum tasks is extensive and includes evaluation of all documentation, performance of requirements interface analysis, design interface analysis, implementation interface analysis, and installation configuration audit. IEEE Std. 1012 does not indicate what these analyses include. Thus, it will be difficult for a licensee to perform a task that is not well defined. Further, it may be best for the designer to perform and document the analyses, with the independent person simply reviewing the documented results. However, DG-1054 does not explicitly allow that flexibility. The DG should rather state that the V&V'er should identify which of the minimum tasks to perform, which tasks to review, and which tasks to witness. This would allow the necessary flexibility and not result in wasted effort. Further, it would seem that this is more in line with the 10CFR50 Appendix B requirements for design verification, inspection, and testing.

DRP - 11 Guides & Manuals

1/0

DG-1055: Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

This DG will provide an endorsement of IEEE Std. 828-1990, *IEEE Standard for Software Configuration Management Plans*, and IEEE Std. 1042,1987, *IEEE Guide to Software Configuration Management*, with certain stipulations.

DG-1056: Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

This DG will provide an endorsement of IEEE Std. 829-1983, *IEEE Standard for Software Test Documentation*. Other than the possibility of inconsistency between IEEE Std. 1012 and 829, no other concerns are noted.

DG-1057: Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

This DG will provide an endorsement of IEEE Std. 1008-1987, *IEEE Standard for Software Unit Testing*. The following concerns to ComEd are noted with this endorsement.

Traditional software development defines "unit testing" as testing at a subroutine or other similar level. This is typically a level of testing that is not documented for QA purposes. Thus, this DG would place us in a position of documenting testing above and beyond the QA program. If we define a "unit" as an individual computer program, then testing would be accomplished as part of requirements based acceptance testing (validation).

Another point of concern is in the arena of the definition/identification of the person performing the testing. The DG requires that the tester be independent of the designer. An inference is made that this is consistent with 10CFR50 Appendix B Requirement 3, Design Control. NQA-1 provides further support to this subject. Requirement 3 directs that design verification be performed by competent personnel other than the designer. The verifier is presented with three choices of activities - design review, alternate calculations, or qualification tests. A combination must be selected. No mandate is made that testing shall be performed by the verifier. IEEE Std. 7-4.3.2-1993 identifies that if testing is done by the designer, the verifier must review the plans, procedures and results. While testing is typically done independently, the mandate of this DG seems to exceed licensing requirements.

Finally, IEEE Std. 1008 is almost 10 years old. The philosophy of development has changed significantly in that time frame. Thus, endorsing this standard seems inappropriate.

DG-1058: Software Requirements Specification for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

This DG will provide an endorsement of IEEE Std. 830-1993, *IEEE Recommended Practice for Software Requirements Specification,* with certain stipulations. A small number of these stipulations are of concern to ComEd.

DG-1058, section 6.3 indicates that requirements for fault tolerance should be specified for each operating mode. The phrase "fault tolerance" may be viewed from two different perspectives - safety system and computer. If fault tolerance, viewed from the safety system perspective, would be indicative of current multiple trip channels, etc. Viewed from a computer perspective, fault tolerance would be a new requirement, as fault tolerant computing has not been considered for safety systems. To properly consider fault tolerant computing, several issues would require resolution. These include additional significant complexity, determination of when to place the channel in a trip condition, and others.

It is recommended that the phrase "fault tolerance," be replaced with "redundancy."

Section 7 notes that sections of the IEEE Std. 830 Software Requirements Specification format which are inappropriate, should be denoted as "N/A." If we are using the standard for guidance, then we should simply not use sections that do not apply. Too much time is spent explaining that a section does not apply, rather than dealing with the applicable sections. This section of the DG should be eliminated.

DG-1059: Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

This DG will provide an endorsement of IEEE Std. 1074-1995, *IEEE Standard for Developing Software Life Cycle Processes,* with certain stipulations. These stipulations are of concern to ComEd.

IEEE Std. 1074-1995 is a prescriptive standard describing a complete set of software life cycle processes. Regulatory Position 2 requires that all mandatory activities be performed, that the requirements described as "shall" are met, and that all the input, outputs, activities, pre-conditions, and post-conditions are described or accounted for in the applicant's life cycle model.

Regulatory position 3 mandates the performance of system safety analyses for each phase of the software development life cycle. It requires that the analyses ensure that no new hazards are introduced. However, there is no explanation of meaning to the phrase, hazards. The ultra-conservative view would be to perform either a MilStd or IEEE hazards analysis. Either of these analyses result in extensive documentation. EPRI research performed at TVA raised questions to the usefulness of the ACEs review required by IEEE Std. 7-4.3.2-1993. Thus, this requirement seems again to be excessive.

As with IEEE Std 1012 (V&V), this specificity and analyses requirements may be appropriate for a digital RPS, ESFAS or an advanced plant design, but it is excessive for a safety related control board indicator or a digital retrofit.

Conclusion

If these Guides are approved without any revision, the ability of the nuclear utilities to implement safety related digital retrofits in a cost effective manner, will be impacted. Compliance with Regulatory Guides is, theoretically, not required. However, deviations from the NRC positions stated in these Guides will most likely receive scrutiny with final digital system implementation, potentially delayed. Thus, issues such as those noted, need to be addressed.

Please feel free to contact this office if you have any questions pertaining to this review.

Sincerely,

John C. Brons
Vice President
Nuclear Support