



RECEIVED

2002 JUL 30 AM 8:50

D. R. Woodlan, Chairman
Integrated Regulatory Affairs Group
P.O. Box 1002, Glen Rose, Texas 76043

Rules and Directives

Branch
(1000)

Ref: DG-1118

STARS-02013

July 19, 2002

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

5/13/02

67FR32069

(4)

**STRATEGIC TEAMING AND RESOURCE SHARING (STARS)
COMMENTS ON DRAFT REGULATORY GUIDE DG-1118
(PROPOSED REVISION 1 OF REGULATORY GUIDE 1.53)
APPLICATION OF THE SINGLE-FAILURE CRITERION TO SAFETY SYSTEMS**

Gentlemen:

The Strategic Teaming and Resource Sharing (STARS)¹ plants have reviewed the subject draft regulatory guide and offer the comments below. We appreciate the opportunity to provide input on this guidance.

1. On page 6, in Sec. 3, TECHNICAL APPROACH, IEEE Std 379-1972 and 2000 sections comparison table, the last item in the IEEE Std 379-2000 Section Number column should read "6.2 and 6.3.1." Section 6.6 does not exist in IEEE Std 379-2000.
2. The last sentence in section "D. Implementation," is confusing. The sentence implies that a licensee must either follow the new version of the RG or the original version. This is incorrect. A licensee may follow its current licensing basis for plant modification, as long as a construction permit is not required. The sentence should be deleted.
3. Section B, "Discussion," second paragraph, last sentence reads: "The single failure could occur prior to, or at any time during, the design basis event for which the safety system is required to function." This position could be interpreted to include so-called "smart failures," which may occur at the most inopportune time during a transient (e.g., a diesel generator successfully starts and accepts automatically sequenced loads upon demand, but fails non-mechanistically at some later time in the event). "Smart failures" (and multiple failures) are often incorporated into licensed operator training programs (e.g., during simulator exercises),

¹ STARS consists of six plants operated by TXU Generation Company LP, AmerenUE, Wolf Creek Nuclear Operating Corporation, Pacific Gas and Electric Company, STP Nuclear Operating Company and Arizona Public Service Company.

Template = ADM-013

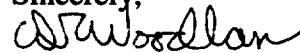
E-REDS = ADM-03
Add = A. Beranek (AFB)
S.K. Aggarwal (GKA)

to build confidence and to focus attention on safety functions, alternate safe shutdown success paths, and recovery options. "Smart failures" are not, however, necessarily consistent with facility licensing bases. One way to classify single failures is as either dependent or independent failures. A dependent failure is assumed to occur upon demand, as a result of the event sequence (e.g., a loss of off-site power following a turbine trip in which the loss of generating capacity may itself render the electric grid unstable). An independent failure is likewise assumed to occur upon demand, but involves a pre-existing failure that becomes self-evident only when the equipment is called upon to function (e.g., a failure of a diesel generator to start and load, due perhaps to a pre-existing leak in the starting air system). It is recommended that the NRC staff reword the sentence to state: "The single failure is assumed to become self-evident upon demand, and may occur prior to, or at any time during, the design basis event for which the safety system is required to function."

4. Section B, "Discussion," second paragraph, item (1), states that safety systems must perform all required safety functions for a design basis event, in the presence of any single detectable failure and concurrent with all identifiable but nondetectable failures. Because a determination of "detectability" is apparently based on an assumption that test results in the presence of the failure would be different from those that would be obtained if no failure was present, this guidance could be particularly difficult to implement for digital protection, control, and monitoring systems that employ software. For example, to what extent can software Verification & Validation (V&V) be credited in a Failure Modes and Effects Analysis (FMEA), to satisfactorily determine that undiscovered software "bugs" do not constitute "identifiable but nondetectable" failures? Are there any examples that the NRC staff would be willing to include in the revised Regulatory Guide?
5. Section A, "Introduction," third paragraph, the sentence "Regulatory Guides are not substitutes for regulations, and compliance with regulatory guides is not required." is repeated twice.

The STARS plants appreciate the opportunity to comment on this draft regulatory guide. If there are any questions regarding these comments, please contact me at 254-897-6887 or dwoodl1@txu.com.

Sincerely,



D. R. Woodlan, Chairman

Integrated Regulatory Affairs Group

STARS