



Westinghouse

12/23/08

73 FR 78856

(2)

Westinghouse Electric Company
Nuclear Services
P.O. Box 355
Pittsburgh, Pennsylvania 15230-0355
USA

Rulemaking, Directives and Editing Branch
Office of Administration
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555-0001

Direct tel: (412) 374-4643
Direct fax: (412) 374-3846
e-mail: greshaja@westinghouse.com

Our ref: LTR-NRC-09-13

February 18, 2009

Subject: Westinghouse Comments on U.S. NRC Proposed Revision 1 of Regulatory Guide 1.62 (DG-1190)

Westinghouse appreciates the opportunity to provide comments to the NRC regarding the proposed revision to Regulatory Guide 1.62 in accordance with the Federal Register Volume 73, No. 247, December 23, 2008. The comments, included in an attachment to this letter, indicate areas of disagreement with the NRC's regulatory position and also provide suggestions to improve clarity. These comments endeavor to ensure that the revised Regulatory Guide effectively communicates guidance with respect to the means for manual initiation of protective actions provided by otherwise automatically initiated safety systems.

If you have any questions or require additional information, please contact either me or Tom Hayes at (412) 374-4420.

Very truly yours,

J. A. Gresham, Manager
Regulatory Compliance and Plant Licensing

Attachment

RECEIVED

2009 FEB 19 PM 4: 20

RULES AND DIRECTIVES
BRANCH

SONSI Review Complete
Template - ADM-013

FRIDS = ADM-03
Cell = K. Nguyen (KHN)

Westinghouse Comments on U.S. NRC Proposed Revision 1 of Regulatory Guide 1.62, Manual Initiation of Protective Actions (DG-1190)

Westinghouse Electric Company is pleased to submit the following comments on DG-1190.

1. There appears to be a significantly expanded expectation for safety-related controls at the component level. The expectation and basis are not clear. For example, the third paragraph in Section B states "..., individual means should also be provided to implement manual initiation at the plant component level..." This appears to be a new Regulatory Position; however, it does not appear in Section C. If this is a new Regulatory Position, Westinghouse believes it is a significant expansion of the existing guidance in Regulatory Guide 1.62, Revision 0, beyond the scope of any requirement in IEEE Std 603. Moreover, it is not clear whether these additional controls are expected to be safety-related. If so, the single failure criteria should be applied at the protective action level (e.g., SI, Containment Spray, etc.), not at the individual component level within each division. If the intent is to add additional controls, added equipment complexity with no clear safety benefit may result.
2. The last sentence of Section B states, "... this regulatory guide focuses on criteria for safety-related equipment of systems and does not address diverse manual-initiation equipment that is not classified as part of a safety system." However, there is a relationship between IEEE Std 603, BTP 7-19, this regulatory guide and the concept of manual initiation of protective actions to cope with software common cause failure. Therefore, it is suggested that the last sentence in Section B be deleted and additional clarification be added.
3. The proposed Regulatory Position C.4 is a misapplication of the principle of diversity as described in Branch Technical Position (BTP) 7-19. The manual controls used to address Point 4 of BTP 7-19 and IEEE Std 603 only confuses the complicated and controversial topic of defense-in-depth and diversity. There is no provision in IEEE Std 603, and its companion standard IEEE Std 7-4.3.2, that precludes the use of digital circuitry in the manual actuation path. Westinghouse believes that the manual system-level actuation path can, and generally should, include digital circuitry. Digital circuitry is more reliable than the alternative discrete analog logic (relays, timers, etc.). Furthermore, Westinghouse believes that requiring the manual and automatic actuation paths to be separate is not the best method to achieve the goal of high reliability.

Section B eleventh paragraph states that, "BTP 7-19 asserts that manual controls for safety equipment should be connected downstream of the plant's digital I&C safety system outputs." This paragraph (C.4) incorrectly interprets the guidance in BTP 7-19 to apply to all manual controls for safety equipment. Therefore, the sentence, "In the case of automated digital protection systems, the point at which the manual controls are connected to safety equipment should be downstream of the plant's digital I&C safety system outputs," should be deleted.

Manual controls that exist to cope with software common cause failure (CCF) of a digital safety system (those addressed in BTP 7-19) must not be susceptible to the same CCF as the digital safety system, and therefore are generally connected downstream of the

digital safety system outputs. There is no requirement for manual controls of safety equipment to be independent of, or separate from, the digital safety system if they are not credited for coping with a failure of the digital safety system.

4. The existing guidance in Regulatory Guide 1.62, Revision 0, Regulatory Position 4 allows that "...action-sequencing functions ... may be common if individual manual initiation at the component or channel level is provided in the control room." This provision is removed in DG-1190. The removal of this provision is not justified.
5. Section B, fourth paragraph, indicates that manual actuation is a backup to automatic actuation. IEEE Std 603 does not require the manual controls to cope with a failure of the automatic actuation. They are simply another method to achieve the actuation. The use of the term "backup" is not appropriate. The term "backup" would be appropriate if describing the manual controls addressed in BTP 7-19. As stated in Item 3 above, DG-1190 is confusing the requirements of IEEE Std 603 and the diversity issues of BTP 7-19.
6. Section B, sixth paragraph, states that "Safety-related controls and displays should be provided." Although it is true that these controls and displays must be provided, this entire paragraph is confusing, adds no value, and thus should be deleted.
7. Section B, eighth paragraph, addresses CCF and Regulatory Guide 1.53. It is recommended that this paragraph be replaced with a simple reference to Regulatory Guide 1.53. This entire discussion on how to address single failures and software CCF is not unique to manual actuation.
8. The words "for each division" have been added to Regulatory Position C.1 (second line) and C.2 (first line). The intent of this addition is not clear. Westinghouse has traditionally provided actuation switches on the control board for engineered safety feature (ESF) actuations and reactor trip. One switch actuates the function in all divisions, minimizing discrete operator manipulations as required by IEEE Std 603, Clause 6.2.1. It appears that these switches should now be designed such that each switch only communicates with one division, thus requiring an operator manipulation for each division for each function. The intent of this change should be clarified; or, the words "for each division" should be deleted.
9. Proposed Regulatory Position C.1 includes the words "..., regardless of whether means are also provided to initiate the protective action at the component or channel level..." These words seem to indicate that component-level control is not necessarily required, further confusing the issue raised in Item 1 above.
10. Section B, third paragraph, states that "manual initiation for each appropriate plant system component (e.g., start pump, open or close valve) is subsequently required..." It is not clear how "appropriate plant system components" are identified. The AP1000 is a passive plant. ESF actuations are automatic and require no further component-level manipulations. Therefore, Westinghouse would conclude that AP1000 has none of these components. Clarify the criteria for identifying "appropriate plant system components."

Westinghouse agrees that high functional reliability is needed. There are many methods to achieve high reliability. Many of these alternate methods provide higher reliability than

simply adding circuitry for manual actuation. Alternative methods to achieve high reliability should be allowed and encouraged.

11. Proposed Regulatory Position C.2 has added the sentence "Multiple initiations of safety systems (autosequencing) by distinct manual control manipulations are not precluded." This sentence is confusing. For example, is "autosequencing" the same thing as "action-sequencing" in the previous sentence? If there is intent to soften the requirement that manual initiation perform all actions performed by the automatic means, then this should be clearly explained.
12. Regulatory Analysis Section 3.2 states "Applicants would incur little or no cost and may, in fact, achieve cost savings." Westinghouse does not agree. If the suggestions in this draft regulatory guide were incorporated into the AP1000 design, specifically the added circuitry for separate non-digital circuits for all manual controls, many additional cabinets for the analog circuitry and their associated costs would be required. The AP1000 is a compact plant design. It is not apparent that the currently-designed buildings can hold these additional cabinets. The added circuitry must also be designed, purchased and installed. In addition, periodic surveillance and corrective maintenance on this additional analog circuitry will be a significant recurring operations/maintenance cost.
13. Section 4, Conclusion, indicates that the primary benefit to the proposed regulatory guide is reference to the modern standards. This proposed revision does much more than update the standards references. There is also a statement that alludes to cost savings. No cost savings have been identified in the draft regulatory guide and Westinghouse can only identify cost increases for these added requirements and added circuitry as indicated above.