Relevant Text from the Staff Requirement Memorandum to SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs"

18. II.Q. Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems:

The Commission **approves**, in part, and **disapproves**, in part, the staff's recommendation. The Commission has approved a revised position, as follows:

1. The applicant shall assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common mode failures have adequately been addressed.

2. In performing the assessment, the vendor or applicant shall analyze each postulated common-mode failure for each event that is evaluated in the accident analysis section of the safety analysis report using best estimate methods. The vendor or applicant shall demonstrate adequate diversity within the design for each of these events.

3. If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.

4. A set of ~~safety grade~~ displays and controls located in the main control room shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in items 1 and 3 above.

The staff's position has been modified in essentially two respects:

First, inasmuch as common mode failures are beyond design-basis events, the analysis of such events should be on a best-estimate basis.

Second, the staff indicates in its discussion of the third part of its position that "The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions." Therefore, this clarification has been added to the fourth part of the staff's position (which refers to a subset of the safety functions referred to in the third part) by removing the safety grade requirement. Further, the remainder of the discussion under the fourth part of the staff position is highly prescriptive and detailed (e.g., "shall be evaluated," "shall be sufficient," "shall be hardwired," etc.). The Commission approves only that such prescriptiveness be considered as general guidance, the practicality of which should be determined on a case-by-case basis.