



Westinghouse
Electric Corporation

Energy Systems

Box 355
Pittsburgh Pennsylvania 15230-0355

NSD-NRC-97-5193
DCP/NRC0922
Docket No.: STN-52-003

June 25, 1997

Document Control Desk
U.S. Nuclear Regulatory Commission
Washington, DC 20555

ATTENTION: T. R. QUAY

SUBJECT: AP600 APPROACH TO SOFTWARE FAILURE ROOT CAUSE ANALYSIS

Reference: 1. Westinghouse Letter NSRA-APSL-93-0213, "Westinghouse Responses to NRC Requests for Additional Information on the AP600," dated June 17, 1993.

Dear Mr. Quay:

As requested by the NRC during a June 9, 1997, meeting in Rockville, Maryland, Westinghouse is formally communicating the AP600 approach to software failure root cause analysis. This supplements the response to RAI 420.101 (Reference 1) which is still valid.

Background

During the February 14-17, 1995, AP600 Technical Specifications (T/S) meeting in Rockville, the NRC T/S Branch requested that Westinghouse include a new administrative program in the AP600 T/S. The objective of this program would be to raise the level of awareness that I&C failures must be carefully evaluated to determine whether the root causes are related to hardware or software. The scope of the program would include evaluating the cause of the inoperability, determining the affected components, and providing plans and the schedule for completing remedial actions. The program, as proposed by the NRC, would also require a special report to be submitted to the NRC within 30 days of determining that a common mode software failure exists.

Approach

This new administrative program, referred to as the software failure root cause analysis program, should not be required since it is redundant with the Quality Assurance Program of 10CFR50 Appendix B Criterion XVI, the requirements already included in the AP600 T/S for determining operability and taking corrective actions, and the guidance provided by NRC Generic Letter 91-18. The Final Policy Statement of Technical Specifications Improvements for Nuclear Power Reactors recognizes the redundancy with the Quality Assurance Program and the desire for T/S simplifications, and therefore does not include a program to determine the root cause of deficiencies relevant to safety as part of the Administrative Programs section of NUREG-1431, which the NRC has required the AP600 T/S to emulate. In addition, the only NRC guidance regarding this issue is Information Notice 93-57 (July 23, 1993) which makes no mention of such a program.

EO 4 1/2

9707070026 970625
PDR ADOCK 05200003
A PDR



10CFR50 Appendix E Criterion XVI

Each Licensee is required to develop a Quality Assurance Program as described within 10CFR50 Appendix B Criterion XVI, which states:

"Measures shall be established to assure that conditions adverse to quality, such as failures, malfunctions, deficiencies, deviations, defective material and equipment, and nonconformances are promptly identified and corrected. In the case of significant conditions adverse to quality, the measures shall assure that the cause of the condition is determined and corrective action taken to preclude repetition. The identification of the significant condition, and the corrective action taken shall be documented and reported to appropriate levels of management."

The result of this Regulation is such that any failure, whether hardware, software, mechanical or electrical, that defines a condition adverse to quality would be evaluated. As part of this root cause evaluation program, one would determine the cause of the failure, the total impact on safety due to the identified cause, and the corrective action to repair the identified deficiency and to preclude repetition of the problem. All failures that are significant to safety would be evaluated to ensure that the cause of the condition is determined and corrective action identified and taken. This includes all failures, not just a select category of failures, and includes failures of I&C systems for possible determination of software related problem.

Final Policy Statement of T/S Improvements for Nuclear Power Reactors

The Final Policy Statement of Technical Specifications Improvements for Nuclear Power Reactors is the result of extensive technical meetings with the NRC and has a goal to simplify the T/S to focus the Licensee and NRC attention on the items that require NRC approval prior to any change by the Licensee. This policy states,

"Implementation of the Policy Statement through implementation of the improved STS is expected to produce an improvement in the safety of nuclear power plants through the use of more operator-oriented Technical Specifications, improved Technical Specification Bases, reduced action statement induced plant transients, and more efficient use of NRC and industry resources."

As a result of this effort, many similar items that had historically been included in the T/S were relocated to more appropriate documents and controlled there by the applicable regulatory requirements. The program to determine the root cause of deficiencies relevant to safety was not included as part of the Administrative Programs section of the Westinghouse STS.

Information Notice 93-57

Information Notice 93-57 discusses this particular issue, stressing the importance of IEEE standards applicable to software verification and validation and of software change controls, but does not recommend a program to address the concerns.

"OPERABLE-OPERABILITY" Definition and NRC Generic Letter 91-18

In the event T/S related instrumentation fails to perform its required functions (for any reason, including software flaws/errors), the cause and corrective action must be determined. If the cause is such that other channels/divisions may have a common mode failure, then the other channels/divisions must be checked. Operability determinations must be made in accordance with the T/S "OPERABLE-OPERABILITY" definition and the NRC guidance provided in Generic Letter 91-18. These operability determinations establish the extent of the instrumentation system inoperabilities and will be made on a case by case basis as is the practice for currently operating plants. LCO 3.0.2 will require compliance with the Required Actions in the event any channel/division is found to be inoperable. (LCO 3.0.2 states "Upon discovery of a failure to meet an LCO, the Required Actions of the associated Conditions shall be met.")

Summary

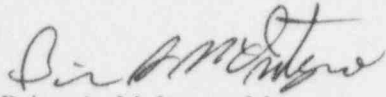
In summary, 10CFR50 Appendix B Criterion XVI establishes the regulatory requirement for a program to identify and evaluate all deficiencies important to safety, which is inclusive of failures in I&C systems. The Technical Specification Improvement Program established criteria for inclusion of items within T/S and allowed the remainder of the items to be relocated to other more appropriate documents and controlled there by the applicable regulatory requirements such that the proposed common mode failure evaluation program was not included as a part of the STS for Westinghouse. Finally, the submitted T/S establish the testing method to determine OPERABILITY of and actions to be taken for individual or multiple situations. As a result, no additional program is necessary to ensure future Licensee attention to potential problems in software based systems.

In developing the AP600 T/S, NRC has allowed deviations from NUREG-1431 only when they are based on AP600 design differences from the PWRs for which NUREG-1431 was initially written. If the NRC feels it is necessary to include a software failure root cause analysis program as part of the AP600 T/S, that position should be accompanied by a technical justification for deviating from NUREG-1431. A digital I&C system is not unique to the AP600. PWRs which have installed the Westinghouse Eagle-21 system have logged years of successful operating with digital systems, without a special software failure root cause analysis program or related addition to their T/S.

The NRC should review this explanation of why no special software failure root cause analysis program is necessary for the AP600 Technical Specifications. This completes Westinghouse action for open item tracking system item 2434 such that the Westinghouse status is revised to "Action N" for NRC to provide feedback regarding the acceptability of the discussion provided above.

June 25, 1997

If there are any further questions or concerns related to this issue, please contact Robin K. Nydes at 412-374-4125.



Brian A. McIntyre, Manager
Advanced Plant Safety and Licensing

jml

cc: W. C. Huffman, NRC
H. C. Li, NRC
M. Chiramal, NRC
M. C. Gareri, NRC
N. J. Liparulo, Westinghouse