D880816

The Honorable Lando W. Zech, Jr.
Chairman
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

Dear Chairman Zech:

SUBJECT: PROPOSED RESOLUTION OF USI A-47, "SAFETY IMPLICATIONS OF CONTROL SYSTEMS"

During the 340th meeting of the Advisory Committee on Reactor Safeguards, August 11-13, 1988, we discussed the NRC staff's proposed resolution of USI A-47, "Safety Implications of Control Systems." This was also the subject of a meeting of our Subcommittee on Regulatory Policies and Practices on August 10, 1988. We also had the benefit of the documents referenced. We had previously discussed the subject during our 336th meeting, April 7-9, 1988, and wrote you a letter dated April 12, 1988, "Proposed Resolution of USI A-47, 'Safety Implications of Control Systems - ACRS Comments.'"

In our letter of April 12 we observed that the scope of the staff work had been "unduly truncated," that there were many relevant subjects omitted, and that the relationship to other USIs was unclear. We therefore concluded that the staff recommendations did not constitute resolution of USI A-47, as originally defined, and recommended that the problem be dealt with by redefining the USI, issuing the proposed resolution as relevant to the newly defined objective, and including the unresolved issues in "a new generic issue, which need not necessarily be accorded USI status."

We commend the staff for its effort to expand its list of the kinds of threats that can be posed by control system failures, though the work remains necessarily and substantially incomplete. Some of the specifics of the omissions noted in our April letter have been addressed, and others have been assigned to the Multiple System Response Program, for which priorities are yet to be set.

We continue to recommend, as we did in April, that this "resolution" be issued, but without any pretense that it is a resolution of the total original concern. We do not wish here to provide a detailed list of

things that ought to be fixed, since that would involve us too heavily in an iterative process with the staff, inappropriate for an advisory committee to the Commission, but will supply some examples of the sorts of issues that require further work.

The procedure used by the staff was, in simplified form, to postulate the failure of an element of the control system, and to perform a Failure Modes and Effects Analysis (FMEA), until one reaches a point in the sequence at which further development is arrested by a safety-grade protective system. At that point, the sequence is presumed terminated. We believe that this takes the regulatory term "safety grade" too literally. The failure probability of a safety-grade system is not zero.

For the most part, as is common in FMEA studies, only failures are considered, with the probability of degradation or misbehavior barely treated. Such questions as the extent to which degradation of a control system can provide incorrect or misleading information to an operator were left untouched, though they were primary factors in our conclusions that control systems represent an important issue.

There are different sorts of failures possible in these areas, and the complexity of possible responses to small disturbances of an electronic system, especially a computer system, is far greater than other sorts of failures. This area of potentially great significance remains largely unexplored. We note parenthetically that the NRC has not made any substantial effort to strengthen its staff capabilities in this increasingly important area. One cannot, therefore, criticize the present staff.

During 1985 the staff issued Regulatory Guide 1.152, "Criteria for Programmable Digital Computer Software in Safety-Related Systems of Nuclear Power Plants," which endorses an ANSI/IEEE-ANS standard. In the Discussion Section in that guide, the staff encouraged the application of this technology "if such advanced technology serves to enhance safety." Thus, the acceptability would appear to require some measure of the new threats that are the inevitable accompaniment of new systems to match against the benefits. The staff recognized in the Regulatory Guide "the unique nature of programmable digital computer systems." In particular, the Regulatory Guide observed that computers are "more vulnerable to subtle failure modes and unauthorized manipulation." This unique feature is not part of the USI A-47 effort. We think it is important.

These concerns do not impel us to change the recommendations in our letter to you of April 12, 1988, as stated in paragraph 2, above. However, we feel it important that the NRC undertake to promptly and systematically broaden its area of expertise to encompass new and increasingly important technological trends.

Sincerely,

W. Kerr
Chairman

References:

1. U.S. Nuclear Regulatory Commission, Draft NUREG-1217, "Evaluation of Safety Implications of Control Systems in LWR Nuclear Power Plants," Technical Findings Related to Unresolved Safety Issue A-47, April 1987.
2. U.S. Nuclear Regulatory Commission, Draft NUREG-1218, "Regulatory Analysis for Proposed Resolution of USI A-47, Safety Implications of Control Systems," April 1987.
3. U.S. Nuclear Regulatory Commission, NUREG/CR-4265, "An Assessment of the Safety Implications of Control at the Calvert Cliffs 1 Nuclear Power Plant," Volumes 1 and 2, April 1986 and July 1986, respectively.
4. U.S. Nuclear Regulatory Commission, NUREG/CR-3958, "Effects of Control System Failures on Transients, Accidents and Core-Melt Frequencies at a Combustion Engineering Pressurized Water Reactor," March 1986.
5. U.S. Nuclear Regulatory Commission, NUREG/CR-4047, "An Assessment of the Safety Implications of Control at the Oconee 1 Nuclear Plant," March 1986.
6. U.S. Nuclear Regulatory Commission, NUREG/CR-4386, "Effects of Control System Failures on Transients, Accidents, and Core-Melt Frequencies at a Babcock and Wilcox Pressurized Water Reactor," December 1985.
7. U.S. Nuclear Regulatory Commission, NUREG/CR-4387, "Effects of Control System Failures on Transients, Accidents, and Core-Melt Frequencies at a General Electric Boiling Water Reactor," December 1985.
8. U.S. Nuclear Regulatory Commission, NUREG/CR-4385, "Effects of Control System Failures on Transients, Accidents, and Core-Melt Frequencies at a Westinghouse PWR," November 1985.
9. U.S. Nuclear Regulatory Commission, NUREG/CR-4326, "Effects of Control System Failures on Transients and Accidents at a 3-Loop, Westinghouse Pressurized Water Reactor," Volumes 1 and 2, August 1985 and October 1985, respectively.
10. U.S. Nuclear Regulatory Commission, NUREG/CR-4262, "Effects of Control System Failures on Transients and Accidents at a General Electric Boiling Water Reactor," Volumes 1 and 2, May 1985.
11. Letter from Victor Stello, Jr., Executive Director for Operations to William Kerr, Chairman, ACRS, Subject: "ACRS Comments on Proposed Resolution of USI A-47, 'Safety Implications of Control Systems,'" dated May 20, 1988

→