UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, D. C. 20555

May 12, 1981

Honorable Joseph M. Hendrie
Chairman
U. S. Nuclear Regulatory Commission
Washington, D. C. 20555

SUBJECT: RESPONSE TO INQUIRY CONCERNING THE SAFETY IMPLICATIONS OF CONTROL SYSTEMS FAILURES

Dear Dr. Hendrie:

In response to a request from Dr. Ahearne in a letter dated December 12, 1980, the ACRS has reviewed the NRC Staff's evaluation of the safety implications of possible interactions of control systems with safety systems. Specific attention has been given the NRC Staff's rationale for concluding that the existing approach for dealing with this problem is adequate until a study can be conducted to determine whether a different approach should be adopted.

We recommended, in a letter of August 12, 1980 to Dr. Ahearne, that control system reliability be added to the list of Unresolved Safety Issues being compiled by the NRC Staff. In that letter we wrote:

> "Recent experience has indicated that more attention must be given to reactor control system reliability. Most safety analyses in the past have given minimum attention to control system reliability based partly on the assumption that failure of the system makes it unavailable and ignores the fact that this failure may actually produce an unsafe mode of reactor behavior. This problem should receive further study to determine appropriate reliability standards for control systems. Appropriate reliability of nonsafety system information displayed for use of the reactor operator is a related important issue."

The NRC Staff subsequently added to its list of Unresolved Safety Issues an item designated "Safety Implications of Control Systems." In the Staff's description of this issue, emphasis was on a study of control system failures that might disable safety systems. In spite of somewhat different descriptions of the problem, we conclude that the NRC Staff and the ACRS agree to a need for further study which may lead to a change in the approach currently used by the NRC Staff in its specifications of the performance to be expected of control systems.

In the course of our review of this question, we have held several meetings with the Staff. We conclude that there is a Staff consensus, based on engineering judgment, that the risk involved in permitting existing plants to continue to operate while further studies are made is acceptable.

It is an accepted precept of control that a single control system cannot be devised with the reliability required to assure protection of a reactor against the spectrum of normal and abnormal events that might be expected to occur. Hence, two systems are provided, one of which, in order to be made as reliable as possible, is comparatively simple, and is required to operate only in emergency situations. In order to decrease the probability that failures in other systems will disable this reactor protection system, it is designed insofar as is feasible, to be functionally and physically separate from the other systems responsible for normal reactor operation.

This separation, reinforced by the assumption that an appropriately designed protection system can protect the reactor against malfunctions of the control system, has led to the current NRC approach that places emphasis on the design and operation of reliable reactor protection systems and much less emphasis on control and other systems.

The accident at TMI-2, and a number of other systems malfunctions that have occurred since, have led to a gradual change in the approach taken by the Staff. In some cases, for example after a study of the importance of auxiliary feedwater systems, this has caused the Staff to reclassify a system from "nonsafety" to "safety-grade." This somewhat piecemeal approach can serve a useful purpose and is appropriate for certain cases needing prompt resolution. In the long run, however, a more systematic approach is needed to determine the appropriate way to deal with the total reactor system.

The NRC Staff reported that a Task Action Plan (A-47, Safety Implications of Control Systems) is being set up to deal with this issue. We believe that a study of this kind on a generic basis is appropriate. We are told, however, that because of other activities which have been assigned higher priority, this issue has not yet received very much attention. We believe that this issue is important enough that within two to three months a program for resolving it should be in place.

The question has been raised as to whether operating plants should be shutdown, should be derated, or should continue to operate at current power levels. We discussed this question with the Staff and also with one Staff member who has recommended that existing plants be operated at 65% of rated power until further studies of control system characteristics are carried out. We found no justification for his choice of derating to 65%, other than engineering judgment, nor was it clear what studies or results therefrom would be required before he would recommend that a resumption of full power operation could be permitted. We do not recommend either shutdown or derating of operating plants.

This most recent examination of the issue of control system reliability and the potential for adverse interactions reinforces the earlier conclusion of the ACRS that a better approach to the specification of control system performance might reduce risk. We therefore recommend that increased priority be

given to the recently designated Unresolved Safety Issue entitled, "Safety Implications of Control Systems" and that the needed resources be allocated for this purpose.

We expect to review and comment on the Task Action Plan as it is developed.

Sincerely,

J. Carson Mark
Chairman