CT-1323

Stephen J. Ditto
CONSULTING ENGINEER – NUCLEAR REACTOR SYSTEMS
3615 Cherrylog Road – Knoxville, Tn 37921
(615) 546-0094

March 4, 1981

Dr. Richard Savio
Advisory Committee on Reactor Safeguards
Washington, D. C. 20555

Dear Dick:

Dr. Kerr requested that we send him comments regarding the Electrical Subcommittee meeting of February 24. This letter is in response to that request.

Although the meeting presented little, if any, new information regarding the design of the CPC, it did provide us with up-to-date information on experience at ANO-2, some insight into the interpretation of that experience by the operators, and an overview of the NRC staff's review plans. My brief comments on these items are intended to present a slightly different viewpoint.

During the meeting the measurement of primary coolant flow was discussed briefly. It was stated that a static flow calibration was made periodically from steam side calorimetry and that dynamic flow calculations were made by the CPC's using pump speed measurements as a major input. It was further stated that there are no installed conventional flow meters, thus the only real flow calibration occurs annually and, if in error, would quite likely involve all protection channels and the control system as well. We have recorded several cases where such errors have occurred and persisted for some time. It is not easy to believe that, in such a system, the core power is known within about 2% as stated in the meeting and that such knowledge is independently obtained from four redundant channels.

The discussion of operating experience at ANO-2 indicated that a number of "bugs" had been found in the CPC system. It was repeatedly stated that all of the failures were "safe" ones. Often these failures caused reactor shutdown - particularly those that involved the CEAC's which are effectively in a one-of-two arrangement. Other shutdowns were caused by

design shortcomings that failed to account for certain power dependent variations. None of these is surprising or alarming. What is surprising (and could be alarming) is that such experience might be taken to indicate that the system failures are all of the "safe" kind. While the mass of evidence points in this direction the conclusion is not justified. It is almost surely true that, in the absence of the need for protective action, the most troublesome failures are the "safe" ones. It is also true that by design, safety systems are frequently super-sensitive. However, it must be remembered that reliability (or safety effectiveness) is not achieved by increasing the number or frequency of "safe" failures but by decreasing the unsafe. Experiencing a large number of easily detected "safe" failures should not delude us into overlooking the possibility of the existence of, or potential for, serious failures of the other kind which are sometimes hard to find.

One last comment is directed at two table presented by Mr. Cogburn of AP&L. The next to last slide presented showed hardware failures and indicated that, of 49 failures, 41 were intermittent and the causes of 16 were unknown. It is my belief that if those intermittent ones had been of the unsafe kind most might never have been detected. Of course the duration of the failure would be a factor. Further, the discovery of the eight "hard" failures would not have been immediate as suggested in the last slide. The point I'm attempting to make is that the probability and timing of detection of a failure in a protection system is strongly dependent upon the nature of the failure. The probability of discovering a "safe" failure almost instantly is very nearly one. Not so with "unsafe" failures. The observed statistics may be telling us this.

Sincerely,

Steve

Stephen J. Ditto
Consultant

cc
Dr. Wm. Kerr, ACRS