OAK RIDGE NATIONAL LABORATORY
OPERATED BY
UNION CARBIDE CORPORATION
NUCLEAR DIVISION

POST OFFICE BOX X
OAK RIDGE, TENNESSEE 37830

CT-1116

PDR 7/13/79

May 7, 1979

Mr. Gary Quittschreiber
Advisory Committee on Reactor Safeguards
Nuclear Regulatory Commission
Washington, DC 20555

Dear Mr. Quittschreiber:

At the close of the meeting on RESAR 414 in Phoenix on March 30, Dr. Kerr requested that we consider what further reviews we think are needed and let him know our views in writing. Although the meeting was primarily concerned with defense in depth, I think it appropriate to restate some concerns I have for the IPS. Some of these have been discussed in detail in previous transmittals to Dr. Savio.[1,2]

Defense in depth is, in my view, compromised considerably by the sharing of sensors among the various "echelons" of defense. While it is clear that one can work around specific and identified failures, the sharing of components in the various lines of defense makes it essential that none of these failures or interactions be overlooked. In addition to the problems of calibration, multiple component failures that involve adverse control and safety interactions, and the like, the IPS testing scheme must alter the operation of the control system so that testing the protection system does not perturb plant operation.

The questions I have raised previously regarding treatment of spatial variations still remain unanswered.

On page 1-5 of NUREG-0493, section 1.2.6 states that overpower can be independently measured by diverse signals such as neutron flux and reactor coolant temperature rise. The degree of independence depends upon how neutron flux channels are calibrated to indicate power. Not only do we find diversity sometimes fictional, we suspect that the control and protection channels are all interlaced via calibration

---

1. Attachment to letter, S. J. Ditto to Richard Savio, July 31, 1978.
2. Letter, S. J. Ditto to Richard P. Savio, August 18, 1978.

methods. The same problem occurs to some degree in conventional hard-wired analog systems now in operation; however, I believe it is even worse when no attempt is made to achieve independence between control and protection systems.

The IPS has a complicated system of automatic bypassing, including some self checking features which can turn parts of the system off and on based on internal decisions. These decisions involve interactions among the redundant channel sets, which are physically isolated but functionally interdependent. There is no doubt that the technology is available to do these things. There is doubt in my mind that the system can be adequately tested and maintained so that failures in these crucial auxiliary operations will not be a problem. In order to achieve high reliability in a system such as this, one must be able to detect and rectify faults when they occur.

The concerns I have regarding the IPS cannot be allayed by hardware and software verification. They are basic to the system. If the system is accepted (and it appears that it has been), I suspect that the detailed evaluation of specifics may require substantial improvements in design over the conceptual design we have seen. The limitations of the signal selector as a device capable of fixing the problem of adverse control-protection interaction will, I believe, be recognized when such an evaluation is made.

It is my understanding that the automatic testing scheme proposes to disconnect all inputs to a channel and replace them with dummy signals, notify the control system to ignore those signals, and inform the other channels that the channel is being tested. With so many automatic alterations of the system functional characteristics taking place routinely, it is not hard to imagine undetected failures that could leave the system crippled in one way or another. This area needs further detailed study.

In summary, it is my view that a detailed evaluation of all parts of the IPS - control system structure will be required when a specific application is made. An audit type of review would not be adequate to uncover flaws that would make the system unacceptable. Any shortcomings discovered at that time could result in costly redesign.

Sincerely,

S. J. Ditto

S.J. Ditto

SJD:fo

cc: Dr. William Kerr

841 164