ELBERT P. EPLER
NUCLEAR SYSTEMS CONSULTANT
712 FLORIDA AVENUE
OAK RIDGE, TENNESSEE 37830
483-0994

Aug 30 1977

Wm Kerr
Chairman Electrical Systems, C&I Subcommittee.

Four recent events have revived interest in a problem of long standing.

1. Arkansas Power and Light is appealing the NRC staff Position 20 concerning the data link between the Core Protection Calculator and the plant computer. It is the staff position that the data link compromise the independence of the protection system.
2. In a recent letter I pointed out that the failure of a d.c. bus would cause impairme of residual heat removal systems and at the same time cause a scram which in turn, would cause d.c. to be needed for residual heat removal.
3. In a recent event at Three Mile Island all four neutron flux power level channels wer miscalibrated by 8 to 10 % for an unspecifie length of time as a result of the failure of a single instrument that provided data for the thermal power computer calculation.

8001170 610 B

4. At Zion in a recent event, dummy signals inserted into the system for test, disabled the shared sensors for protection and control. As a result the vessel water level was lowered by the control, while at the same time the protection against the event was disabled.

Each of these comes under the heading of Separation of Protection and Control, which is poorly understood and in need of attention.

The principle of Separation of Protection and control was established many years ago during the design of the MTR, which was the forerunner of all LWRs. For that reactor a high performance power level controller was applied which was capable of very fast response. A failure of the controller could put the reactor on a severe power excursion and for that reason a high performance protection system was applied. As a minimum the protection system would be required to protect against any event which might be caused by failure of the control. It was perfectly obvious that the systems must be completely separate and independent. Failure of both as the result of a single event would be intolerable.

The principle of separation was clearly logical and sound and continued to be applied to ORNL systems. About 1950 another important reason for separation made an apperance.

An in-pile experiment was presented for review which proposed to use a single instrument both for data collection and for protection of the experiment and the reactor. A high degree of accuracy was desired for the data collection which would require frequent calibration of the instrument. During calibration it would be disconnected from the protective feature in order not to scram the reactor. To calibrate the recorder door would be opened which operation would disconnect the scram feature and at the same time start a timer. The operator would as a result be allowed a limited amount of time for calibration with the experiment and the reactor unprotected. Closing the door would restore the protection.

It was immediately clear that in using the same instrument, or set of instruments, for both functions, the protection would be degraded to obtain accuracy for the experiment, which was totally unneeded for protection. We should be grateful to the experimenter for recognizing the significance of this and leveling with us.

In 1958 an event at HTRE 3 further confirmed the importance of separation. A set of three ionization chambers served both the protection and control system. At some time R.C. noise filters were inserted in the chamber power supply circuits which inadvertantly limited the available current to an amount insufficien to produce a scram. It is not known whether this filter was intended to improve the performance of the protection or of the control. In either case the filter limited the current thereby causing the controller to see a low power level and dutifully withdraw rods to increase the power. At the same time the protection also saw the low power level and did nothing. As a result core melting occurred.

The above illustrates the need for separation to prevent a common mode failure from causing both protection and control to fail. Above all the common mode failure must not result from improvements made to the control system which would cause failure to protect.

The Standard IEEE 279 addresses the problem but fails in an important respect. The same devices may be used for both protection and control providing "the remaining redundant protection channels shall be capa

of providing the protective action even when degraded by a second <u>random</u> failure." This position was adopt to accomodate industry practice where the same device in two of four logic. were invariably used for both protection and control. As a result protection is provi against random failure, which has never been a proble and no protection is provided against common mode failure which is the real problem.

The CRBR took refuge behind the shelter of IEEE 27 in spite of the prohibition contained in RDD standard C16-1. In the primary protection system the same ionization chambers were used for both protection and control. The "diverse" secondary system also measured neutron flux by means of fission counters. For each channel both the chambers and counters were mounted behind a single moderator block which could become contaminated and at the same time cause the failu of the control system and <u>both</u> protection system. Neither system contained a truly diverse thermal power measurement to protect against this event.

The Westinghouse produced line routinely uses the sam instruments for both protection and control. This practi was challenged in 1967, but because of the large amount of diversity in these systems no case could be made for

correction. The following however is contained in my Jan 24, 1969 letter to the ACRS.

"The use of the same or identical but separate equipment for protection and control tends to degrad the protection function and at the same time prevents the use of diversity in control and protection. The use of separate and diverse systems is clearly needed to obtain the required performance.

.... It is the current practice in PWRs to cu off system letdown flow on occurrence of low pressurizer level. Thus a spurious indication of low pressurizer level will be the cause of overpressuriz the system. In this kind of situation where information is contradictory, correct operator respo cannot be counted on.

It is concluded on the basis of the assumed tolerable frequency of uncontained excursions and the estimated excursion rates, that existing techniques are adequate to produce protection features satisfactory for the infrequent primary rupture, t dual and diverse reactor protection systems will be required, and since all protective features are at best, marginal in failure probability, interactions between protection and control must be minimized."

Although the "spurious indication of low pressurizer level will be the cause of overpressurizing the system" was seen as a possible result of using the same devices for protection and control, it was not forseen that a similar condition could be brought about by the use of dummy signals, as was the case at Zion.

Largely as a result of the weak requirements of IEEE 279, the principle of separation has now degenerated to no more than the use of light pipers as evidence of concern. Modern solid state devices are susceptable to stray voltages and precautions are taken to transmit all signals between protection and control through light pipers. In older systems the conventional relays and switches were adequate as isolating devices. No failure is known ever to have occurred because of this problem although it is now receiving attention to the exclusion of the real problems.

In the matter of the data link between the CPCS and the plant computer, I had not taken a position in opposition It is indeed true that signals taken from the protection system to the plant computer can be quite useful in enhancing safety. There is of course the concern that the safety function could be degraded as the result of changes do hardware, or software intended to improve the quality

of the data transmitted to the plant computer. It would seem reasonable that suitable precautions could be taken to prevent this and that the advantages might outweigh the disadvantages.

Recent events however have convinced me that we are virtually without protection against the ill effects of interconnecting the CECS and the plant computer. The true nature of the problem is so little understood that we can not be assured of an adequate defense. We are at the mercy of a few highly specialized computer technicians for assurances that harmful interactions will not result; we have no assurance that they are acquainted with the true nature of the problem. This is borne out by the following taken from the attachment to the letter J. D. Phillips to R Boyd, 7/29/77.

"The data links between the DNBR/LPD Calculator System and the plant computer satisfy the requirements of GDC 24 and IEEE 279-1971, Section 4.7, regarding independence of protection systems. IEEE 279 requires that the transmission of signals from the protection system be through isolation devices. Optical isolators at both sending and receiving ends of the plant computer data links meet this requirement. These optical isolators ensure that no credible event at the plant computer can degrade

the protection system. GDC 24 requires separation of protection and control systems to the extent that failure or removal of common equipment leaves intact sufficient equipment to meet all protection system requirements.

This paragraph provides ample evidence that no effort is contemplated to ensure against more subtle interactions such as harmful alterations to the CPCS hardware, which might be made in order to enhance the quality of data transmitted to the plant computer.

Other vendors will shortly be proposing similar systems having similar problems. I propose that the applicant be required to provide evidence that precautions beyond the requirements of IEEE 279 and GDC 24 have been given consideration.

E P Allen