CT -1321

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

Sanibel Feb 27, 1981

Wm Kerr, Chairman
Electrical Systems Subcommittee

The presentation of cpc operating experience at the Feb 24 subcommittee meeting has disclosed an important problem deserving of careful consideration. The vendor has elected to apply the cpc to protection, whereas there are compelling arguments supported by operating experience, for applying the digital system to control. The issue was touched upon at the meeting, but the treatment was far from adequate.

The cpc is a powerful tool with calculational capability to look at the core in detail with respect to control rod position, flux shape and linear heat rate, thereby permitting operation at the highest possible safe level. Although applied as a protective feature, the trip initiated by the cpc is at a power level somewhat below the trip point of the conventional protection system which has been retained to back up the cpc, and remains capable of protecting the core in the event of cpc failure.

It would appear that any deviations from normal conditions, discoverable by the CPC, could be corrected either by a prompt moderate control action, or by a scram resulting in complete plant shutdown and requiring 24 hours for recovery. The latter course has been chosen, whereas there are compelling arguments favoring reexamination of the matter before approving widespread application of the CPC.

The operating record of the CPC as presented at the subcommittee meeting has given some insight as to the effect on both plant availability and safety resulting from the narrow margin between the operating power level and the CPC trip point. ...

The effect on availability can be seen in the 8 scrams in 220 days of commercial operation, or 27 days per scram. This rate is confirmed in 1981 with two scrams in 50 days or 25 days per scram. These were initiated by the CPC, and half were valid and half spurious. Virtually all of these, whether valid or spurious, were related to distortions of the axial flux shape as would be caused by a dropped rod. This degree of sensitivity to axial shape must be attributed to the small safety margin, i.e., the margin between operating level and CPC trip.

Ten scrams in 270 days would amount to 13 scrams per year. We were told that scram recovery requires 24 hours so that the effect on plant availability would be 292 hours or 4%. The HFIR, a production reactor at ORNL has an availability, including refueling, of 93%. More than one hour per year unavailability attributable to the protection system would be unacceptable.

Although the effect on availability is clearly measurable, the effect of the small margin on safety is more difficult to evaluate. One manifestation of this effect was clearly exposed at the subcommittee meeting. The NRC had directed that the data link connecting the plant computer to the CPC, be disconnected ten days after completion of start up testing. Only now is the NRC aware that the data link remains operational, and its continued use is intended.

The data link is useful for intercomparison of redundant channels to discover a deviation on the part of an individual channel which would be an indication of incipient failure. It is clearly undesirable that the CPC remain dependent on this single component, which in some degree compromises channel independence, so

that it seemed appropriate to ask why its continued use was necessary. It developed that the plant computer provided the only means of detecting normally occurring instrument drifts, usually called "set point drifts". Drifts in the safe direction, not otherwise detected, would result in channel trip, but drifts in the unsafe direction, if undetected would result in degradation or loss of protection.

The degree of degradation was not discussed but should be explored at some future time. This, however, clearly demonstrates that the small safety margin makes the CPC in some degree dependent on the plant computer. This therefore leaves us with a problem. The NRC order to disconnect the data link still stands, but to do so in the face of this known dependence would not be prudent. An alternative would be to derate the plant and thereby increase the safety margin, but this would be highly objectionable. Another alternative, equally objectionable, would be to classify the plant computer as "important to safety" or "safety related" or even "safety grade", put it in a seismically qualified controlled environment and subject it to intensive regulatory review.

The NRC has required that a qualified consultant be employed by the licensee to review software changes. The discussion of this matter made it clear that it is difficult to verify that alterations to software have not impaired protection. There is no simple go, no-go gauge, in fact the effect of changes to software would be comparable to changes in core characteristics. Whereas changes to the core would not readily be made, and would be subject to review, changes to software could be made easily and frequently, and even by accident as a result of human error. The control of software alteration will require continued surveillance, both on the part of the licensee and the NRC.

...

We are at the threshold of expanded application of the CPC, and now have almost a year of commercial operating experience, which has disclosed areas of concern. The narrow safety margin visibly impairs availability, and surely impairs protection, but by an uncertain amount. We have no clear understanding of the existing margin, nor are we aware of criteria governing margin. This is a sensitive matter in that safety and economics are in direct conflict.

Failures detected to date have invariably been safe failures. Both the licensee and the NRC have taken the position that virtually all failures would be in the safe direction. This is entirely unbelievable, however if this position is maintained we should extend an invitation to demonstrate its validity.

The rate of 13 scrams per year is unacceptable to the licensee, and measures are being adopted to improve the situation. We should be alert to the danger of improving availability at the expense of safety, and should allow no unnecessary obstacles to impede this effort. Such unnecessary impediment has, however, made an appearance.

...

The vendor attempted to have the four channel protection system accepted and licensed as a two-of-three system with an installed spare. The installed spare would have economic value only, and would permit greater flexibility in designing features to minimize the occurrence of spurious scrams. The NRC has taken the position that the two-of-four configuration must be maintained, and has thereby impeded the effort to improve availability. This could increase the incentive to improve availability at the expense of safety. The staff should be invited to defend this position.

The above discussion leads to the following conclusions.

a. A scram requiring 24 hours for recovery is a severe penalty for the relatively unimportant deviations discovered by the CPC. A prompt corrective control action would be more appropriate.

b. The CPC is an exceedingly complex system, completely understandable to only a few specialists, yet it must be intensively and continuously reviewed. This can only increase the time and effort for licensing, whereas a reduction in licensing effort is being demanded. By inclusion of control rod position and flux shape and other useful features, the scope of performance has been broadened to the point that protection capability has been significantly diluted.

c. The loss of availability caused by small deviations in control nullifies much of the economic advantage to be expected of the digital application, and the gain in protection is not clearly apparent.

d. The function of the CPC is typical of control yet the system must perform while encumbered

by the requirement for four channel redundancy and other requirements imposed on protective features, eg, the troublesome one-of-two vod position data.

e An important consideration is the relative consequence of control vs protection failure. Protection system failure at an observable rate would not be acceptable i.e., an acceptable rate of 10^{-5}/yr, would not be observable. Control failure, on the other hand, would result only in a challenge to the protection, and in plant shutdown. The rate of failure should be readily observable, and the economic penalty would encourage the licensee to take steps to minimize the failure rate, which he should be encouraged to do with minimum regulatory participation.

At ORNL the decision was made in 1947 to interpose a control correction to intervene and prevent a given variable from reaching the scram point, whether the excursion were real, or no more than instrument drift. A third of a century of operation has confirmed the validity of that decision. HFIR availability is 93% including complete

refueling every 23 days, and during the two hundred reactor years of operation at ORNL since 1947, there has been no known instance of a scram being needed to avert core damage.

The CPC operating record leads only to the conclusion that it would be better to design the control system to promptly respond to small and relatively frequent deviations, and to reserve protective action for defense against larger and relatively infrequent excursions. The existing system falls short of optimization of the effort expended in prevention, i.e., control vs mitigation, i.e., protection. This being true, the protection thus obtained can not be optimum.