D870115

The Honorable Lando W. Zech, Jr.
Chairman
U.S. Nuclear Regulatory Commission
Washington, DC 20555

Dear Chairman Zech:

SUBJECT: ACRS RECOMMENDATIONS ON IMPROVED SAFETY FOR FUTURE LIGHT WATER REACTOR PLANT DESIGN

During the 321st meeting of the ACRS, January 8-10, 1987, we completed our discussion of improved safety requirements and objectives for future light water reactor power plants (LWRs). This discussion began during the 316th ACRS meeting, August 7-9, 1986. The scope of our present comments is limited to nuclear power plant design. Other factors, such as plant operation and management, are necessarily involved, but are beyond the scope of our present remarks.

The ACRS has on several previous occasions recommended that future LWRs should be designed to be safer than current LWRs. This is not to ignore the excellent safety record thus far of LWRs in the United States. We believe this increased safety can be achieved with reasonable economy because better technology is available today. Improved concepts for plants and improved understanding of risks have been developed over a generation of experience in design, operation, and analysis. But, not all of these concepts have been incorporated into the newest reported LWR designs. We believe many of these concepts can be incorporated with acceptable effect on plant cost or operating efficiency. With the expectation that future plants will be standardized, the next group of plants to be licensed will probably set the safety design philosophy, and even details of implementation, to be used in nuclear power plants for several decades.

The mean estimates of risk from generation of electricity by the use of nuclear energy are at least as low as those for generation by other methods. However, the acceptability of these estimates is much affected by the large uncertainty associated with them. A compelling reason for implementing improvements -- apart from the fact that improvements are possible -- is to reduce the uncertainty in the risk estimates.

Future plants should be able to survive a wider spectrum of off-normal challenges and mistreatments. For example, normal operating systems should be forgiving of most operational errors and imperfections in maintenance. Accident management and mitigation systems should be designed, not for a narrow set of design-basis accidents, but to reasonably accommodate a broad range, variety, and time sequence of threats.

Our recommendations are based on insights provided from quantitative risk analyses, lessons learned from operating experience, and continuing concerns. In the sections that follow, we list and discuss a

number of possible safety improvements. Several of these overlap, and we do not expect that all of them should be implemented. Rather, we offer them with the belief that each is worthy of serious consideration in connection with future designs.

1. Dedicated and Protected Decay Heat Removal System (DHRS)

   We recommend for consideration that future LWRs include a dedicated, protected, redundant, decay heat removal system having its own power, fuel, and water supply, with a capability for makeup, including coolant lost from very small LOCAs, and for recirculation from the containment sump. This system should have a large seismic capability such that its function is not threatened by earthquakes having an occurrence likelihood in the range 10 to 10 per year. There should be similar protection and seismic capability for the primary system and all components whose specific function is required for proper operation of the dedicated decay heat removal system, as well as protection against fires, flooding, and adverse environmental effects. This system should be capable of actuation but not termination from the control room.

   We list this item first because the provision of such a system would alleviate our concerns in several areas, including the following:

   ~ If the DHRS is protected against fire, internal or external floods, sabotage by an insider or by terrorists, and earthquakes at the 10 to 10 probability level, the degree of protection required of other portions of the plant against such events could be relaxed in many instances. In addition to the economies these reductions might lead to, we believe that they might lead to relaxation or removal of many of the impediments to access and flexibility of operation that are now imposed by security and fire control.

   ~ The loss of all sources of AC power, both off-site and on-site (station blackout), would be of less concern if a DHRS is provided. However, vital DC power and certain vital cooling functions (such as cooling of primary pump seals in a PWR) now performed by using AC power would have to be dealt with appropriately.

   In some of the further recommendations that follow, we indicate that the identified needs would be reduced, or perhaps eliminated, if a dedicated, protected, decay heat removal system were provided.

2. Safety Train Redundancy

   The general principle of "N+2" trains should be adopted for active, safety-related functions. N is defined as the number of trains required to perform a necessary safety function. N is equal to one if the train has 100% capacity to perform the function. N is equal to two if each train has 50% capacity. Thus, an "N+2 rule" would require three 100% trains, or four 50% trains. Each of the N trains would have its own independent

support systems. Each train would be physically separate from the others, and diverse designs or equipment should be considered if this can be shown to provide a significant safety advantage. Exceptions to this general principle should be permitted for systems providing functions with low risk potential and for systems which can be demonstrated to be exceptionally robust and reliable.

The proposed high level of functional capacity could be used to improve plant availability by use of Technical Specifications which permit one of the extra trains to be out of service for maintenance and testing for somewhat longer periods than is now the practice for the first train of redundancy.

3. Design of Containment Systems

The need to mitigate the consequences of certain severe accidents should be considered explicitly in the design of containment systems (structures, penetrations, sprays, vents, etc.). The severe accident sequences to be considered should be those for which the mitigation provided by the containment systems is required to meet the Commission's proposed general performance guideline that the overall mean frequency of a large release of radioactive materials to the environment from a nuclear power plant accident should normally be less than 1 in 1,000,000 per reactor year of operation. The severe accident sequences that need not be considered are those of sufficiently low probability that the releases, unmitigated by specially designed containment systems, will in the aggregate not exceed this objective.

4. Protection Against Sabotage

We are not of one mind on the issue of the extent to which LWRs should be protected against the threat of damaging sabotage by terrorists and insiders.

On the one hand, there is reason to believe that certain design choices can lead to inherently better resistance against such a threat, even if these choices are not specifically directed against sabotage. For example, control rooms can be positioned so they are away from the exterior ground level and protected from truck bombs by existing massive concrete structures. Good physical separation of redundant safety trains may provide significant inherent protection. Some of us favor hardening, or separation, or other protection of most vital functions such that they are relatively well protected against transportable explosives. If included in the original design, part of these changes should result in modest added cost or modest loss of other beneficial plant characteristics.

On the other hand, some of the members are not convinced there is reason to believe nuclear power plants are particularly attractive targets for saboteurs. If a terrorist aims to actually cause injury to large numbers of the public, there are far easier and more effective targets throughout the country. Also, with 120 operating plants [today's population] built to a lower level of sabotage protection and a new set of plants built to a higher

level of sabotage protection, this discrepancy will surely be noted and taken into account by a terrorist in the selection of a specific target, if the aim is to cause physical harm to the public. It appears to these members that the resources society allocates for defense against terrorism would be more effectively used in areas other than nuclear power.

In the case of the insider, the ACRS believes the threat is of low probability. This should not, however, discourage prudent design features which could impede insider actions or reduce the likelihood of success.

5. Fire Protection

Those responsible for conducting probabilistic risk assessments (PRAs) have not been very successful in quantifying the risk from large fires involving essential reactor systems. As a result, the real benefit of existing fire protection provisions and backfits remains uncertain. We believe future LWRs should be designed so that cold shutdown of the plant using safety-grade equipment can be accomplished quickly (within 24 hours) in the event of any single fire which may burn up to 3 hours. Physical separation and protective barrier or compartment arrangements should include a reasonable accounting for the adverse effects of the spread of heat and the products of combustion beyond the fire zone, including consequential spurious actuation of fire mitigation features and the resulting damage to safe shutdown equipment. Fire mitigation features should be designed to function properly, and not to spuriously actuate, during or after a seismic event.

If the plant has a DHRS as discussed above, only those other portions of the plant vital to accomplishing safe shutdown would need to be protected against fire consistent with the more stringent requirements listed above.

6. Anticipated Transients Without Scram (ATWS)

We suggest that design features be introduced that would make an ATWS event a much less serious, if not a negligibly small contributor, to risk. For PWRs this might involve some combination of increased negative moderator temperature coefficient of reactivity and increased pressure-relieving capability for the primary system. For BWRs a partial contribution would be made by something approaching 100% relief capability in the event of turbine trip or main steam isolation valve closure. We also suggest that the combination of control and safety systems be examined for reliability, as well as for testing and maintenance of the systems, to reduce the need for some of what are now considered to be safety-related scrams, as well as to reduce the number of spurious scrams.

7. Systems Interactions

Operating experience and reviews of existing nuclear power plants have provided evidence of unanticipated adverse interactions from supposedly separate systems. These supposedly separate systems

sometimes interact in unanticipated ways because they are dependent on common support systems (such as power supplies, common piping systems, etc.) or because they share the same or adjoining physical space. Those people responsible for performing PRAs can successfully incorporate the effect of these interactions only if they are known and understood and if probabilities of occurrence can be established. We believe that further effort is warranted to develop techniques and processes which can seek out and eliminate such interactions.

8. Electric Power Systems

We believe that the frequency of transients and spurious reactor scrams should be reduced by providing electric power supplies that are less vulnerable to transmission network disturbances. We recommend that General Design Criterion 17 be revised to require that the circuit which is provided to be immediately available to cope with a LOCA be the normal power supply to the plant auxiliaries and safety systems and be supplied continuously and unswitched from the low side of the main stepup transformer during and throughout startup, operation, and shutdown of the nuclear generating unit.

We believe that the capability of a plant to cope with the loss of all off-site power can be improved. For one thing, the proposed resolution of Unresolved Safety Issue A-44, Station Blackout, should be implemented in the design of future plants. For another, the reliability of on-site AC power sources can be enhanced by designing the nuclear system with sufficient steam bypass, feedwater inventory and make-up, and run back capability to sustain unit load rejection from 100% power and to run back to "house" electrical load, or by providing an additional, preferably diverse, standby electrical generating unit. The need for these features would be reduced if a DHRS is provided, as discussed in Item 1 above.

9. Probabilistic Seismic Design

Important safety systems should be explicitly designed using probabilistic seismic design methodology to survive and function during and after severe seismic events. Only survivability and those functions needed to bring to and hold the reactor at cold shutdown need be considered. A DHRS such as discussed above would reduce the number of structures and systems requiring very stringent seismic design.

10. Primary Pressure Boundary

We recommend that the primary system pressure boundary be designed and fabricated to minimize the number of welds and optimize the ease of inspecting them.

11. Dedicated Systems and Sharing

There should be minimum sharing of equipment, flow paths, and support facilities among nominally separate systems.

12. Control Room Protection for Severe Accidents

Safe habitation of the control room and other necessary facilities should be ensured in the event of an accident that results in a large release of radioactive materials outside containment. For multi-unit sites, this requirement applies to both the damaged unit and other units on the site.

Additional comments by ACRS Members H. Lewis, F. Remick, P. Shewmon, and D. Ward are presented below.

Sincerely,

William Kerr
Chairman

Additional comments by ACRS Members H. Lewis, F. Remick, P. Shewmon, and D. Ward.

This is a camel of a letter, describing a camel of a reactor. We have no reason to doubt that each of the features recommended in the letter may improve safety, nor do we have any reason to believe that there are not better and more cost-effective alternatives. This problem is compounded to the extreme by putting them all together.

The purpose of this letter is presumably to distill the Committee's observations and experience with the current generation of reactors, designed over the last few decades, and to put that experience to work in expressing a design philosophy for the next generation of reactors. There is no hint of a philosophy, but instead a laundry list of improvements, all unanalyzed. Though the Committee has often recommended that the next generation be safer than the past, that recommendation has never been justified. It may be right, but seems to be inconsistent with the Commission's Safety Goal Policy. There is no doubt in our minds that, with new technology and years of experience, a new generation can be either safer at comparable cost and level of complication, or equally safe at lower cost and greater simplicity, and that choice is so fundamental that it is, in our view, not responsible for the Committee to opt for greater safety and greater complication without analysis or justification.

We believe one can learn from experience and that the next generation must inevitably be better than the past (and thereby safer), but we are uncomfortable about designing those reactors in committee.

Additional comments by ACRS Member, David A. Ward.

I disagree with the Committee's recommendation that future LWRs should include a dedicated, bunkered decay heat removal system. In my opinion, the safety advantage from such a system is highly uncertain

and likely to be very slight or even negative. The cost would be great and there would be added complexity in operations. I believe added reliability offered by adoption of the N+2 principle with some diversity and separation of trains is adequate and preferable.

The promises of trade offs, e.g., relaxation of requirements on main-line systems, are phantoms. A systematic study to determine what should be included in a bunkered system and whether there would indeed be important trade offs might be warranted at this time, but the Committee has not made such a study. The recommendation is a hip shot.

The Committee has elected not to make recommendations relative to either of a pair of weaknesses in LWRs which I believe make them the object of criticism from the proponents of new reactor concepts. These are: 1) absence of a backup scram system and 2) the fact that every scram, real or spurious, becomes a challenge to the plant because of the necessity for emergency feedwater. I believe consideration should be given to development of an independent backup scram system for LWRs. This would include not only independent sensor and control logic, but also an additional system of absorber rods or other material (possibly a liquid) to rapidly and reliably enter the core. Further, I believe there should be consideration of a passive or continuously operating decay heat removal system so that a reactor scram will not be a challenge, but instead always be an unambiguous shift to a safer operating mode.

Beyond these two specific points, I believe the best approach for the NRC to take in implementing safety improvements, such as those suggested in this letter, in LWRs of the future is to incorporate them into a revised set of General Design Criteria. Although iteration with designers and licensees will be necessary, the improvement process will best be served by establishing a clear new basis at the beginning.

In addition, I am concerned that the concept of quality assurance, as applied in the nuclear power industry, has not been successful. I do not, of course, question the need for quality nor do I have major concerns about the quality of existing plants. However, I do question whether QA has had much to do with either. This might not be so troublesome except that QA as practiced is very expensive and uses resources that might better be spent in other activities, including more effective reactor safety programs. I suggest that the present hiatus in plant design and construction provides an opportunity for the Commission to rethink its commitment to the present concepts and practices of QA.

→