D880720

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

Dear Chairman Zech:

SUBJECT: REPORT ON KEY LICENSING ISSUES ASSOCIATED WITH DOE SPONSORED REACTOR DESIGNS

During the 339th meeting of the Advisory Committee on Reactor Safeguards, July 14-16, 1988, we met with members of the NRC Staff and the Department of Energy (DOE) Staff and reviewed a draft Commission Paper on "Key Licensing Issues Associated with DOE Sponsored Reactor Designs," dated February 9, 1988. This subject was also considered during our 334th, 335th, 336th, and 337th meetings on February 11-13, 1988; March 10-12, 1988; April 7-9, 1988; and May 5-7, 1988, respectively. Our Subcommittee on Advanced Reactor Designs met on January 6, 1988 to discuss this matter. We also had the benefit of the documents referenced to this letter.

The Commission, in a letter dated July 9, 1987, instructed the staff to develop such a key-issues paper in advance of projected safety evaluation reports on each of the three conceptual designs being proposed by DOE and its contractors. The Committee believes this was a wise decision; it is appropriate to confront and attempt to resolve the most important safety and licensing issues in a general and direct way, rather than only by reacting to design proposals. In doing this, the NRC Staff has undertaken an important and difficult task. It can be viewed as an attempt to create, from the top down, a comprehensive rationale for licensing requirements. This would be very different from the existing body of regulations for light water reactors (LWRs), which has grown an element at a time in a more reactive and pragmatic fashion.

The nation has more than thirty years of experience in the development and realization of practical nuclear power. The DOE sponsored designers have made use of this experience and of associated research and analytical development to create three conceptual designs which they believe offer significant advantages over existing LWR plants.

Similarly, the NRC should take advantage of experience in the regulation and safety analysis of plants to create an improved approach to the specification of safety requirements. In doing this, care must be taken that regulatory requirements do not unnecessarily frustrate the development of advanced reactors. The regulations should permit the application of innovative reactor concepts while protecting the health and safety of the public. We believe this can be done, but additional effort on the part of the Commissioners and the NRC Staff will be required. False urgency should be avoided; it is more important to do the job right than to do it soon.

The staff effort so far has been thoughtful and productive, and provides appropriate preliminary guidance. They have identified four key issues as a basis for review of the design proposals:

~ Accident selection

~ Siting source term selection and use

~ Adequacy of containment systems

~ Adequacy of off-site emergency planning.

We believe these are important issues, but they do not adequately encompass the full set of concerns. We comment below on these issues and then discuss several additional issues that we believe are also important and deserve further development. We suggest that the staff's key-issues paper be regarded as preliminary guidance and that a continuing program of development and dialogue is necessary before criteria are considered final.

ACCIDENT SELECTION

The staff has proposed four event categories for selection of design basis events based on estimates of the probability of events that might challenge a given system and on past practice and engineering judgment.

For the second of these event categories (EC-II), the staff would require that there be tolerance for single failures, that only safety-grade systems should be credited in meeting the event challenge, and that reactor plant systems should continue to operate normally in response to the challenge. We believe this general approach is sound, but requires two caveats:

~ Credit for performance of nonsafety grade equipment in this class of events should be permitted when this can be justified. Designation of a component or system as safety grade is intended to ensure it has certain specific attributes. Among these are the ability to resist certain seismic events, ability to function within certain harsh environments, and a high level of reliability (supposedly guaranteed by a quality assurance program). Not all postulated initiating events are challenges to all of these attributes. Selectivity should be permitted when sufficient information is available about the nature of the design basis event.

~ We agree there should not be complete dependence on probabilistic arguments. Although estimates of probability are a proper first-cut approach to the definition of event categories, uncertainty in these estimates is large. Judgments are needed about whether and how to include as design criteria the capability to accommodate phenomena and sequences that are not specifically indicated to be necessary by probabilistic estimates.

CONTAINMENT SYSTEMS

Containment structures clearly are intended to restrict release to the environment of radioactive materials resulting from a severe accident. For LWRs, although the design bases for containments have included a source term related to severe accidents, the design pressures and temperatures have been those related to a large-break LOCA rather than those resulting from an accident involving severe core damage. Whether this seemingly inconsistent but pragmatic approach has served the nuclear power enterprise well can be debated. On the one hand, some of the severe accident issues facing the NRC and the industry today are a legacy of that approach. On the other hand, such a containment performed very well in the TMI-2 accident. Research over the past few years indicates that most existing containments would be reasonably effective in reducing the consequences of severe accidents.

The staff proposal for severe accident and containment requirements for advanced reactors seems to be taking a different, but not necessarily better approach, than that used for LWRs. Their contention is that, if the early lines of defense, namely:

- prevention of challenges to protection systems, and

- prevention of core damage by protection systems

are effective enough, then the next two lines of defense, namely:

- a conventional containment structure, and

- an emergency plan for the area around the site,

are not necessary.

The so-called prevention and protection attributes of the three designs being proposed by DOE and its contractors are indeed impressive. The modular high temperature gas cooled reactor (MHTGR) has no conventional containment structure, but relies instead on the capacity of its unique fuel particles to retain fission products, even at abnormally high temperatures, with high reliability. The two liquid metal reactor (LMR) designs have containers around the reactor vessels, but these have low volume and pressure capacity. It is unclear how they would accommodate a challenge greater than minor leakage of sodium coolant.

Accidents can be postulated that would challenge the defense-in-depth concepts being advanced. For the LMRs, a contemporaneous failure of the guard vessel and the reactor vessel, coupled with a sodium fire, would seem to lead to severe consequences. For the MHTGR, a fire in the graphite moderator, perhaps permitted by massive failures of the reactor vessel and core support, might also have severe consequences. Whether these or other accidents could be effectively mitigated by a containment enclosure, or a filtered vent, has not been determined.

We note that in all three designs, absence of containment helps to make feasible one of the major safety advantages, passive systems for removing decay heat. In each case, the reactor vessel surroundings are designed so that air from outside the plant will flow by natural buoyancy through the reactor vessel cavity and thereby remove decay heat. This seems to be a highly effective heat transfer means if the reactor vessel and core are intact. If they are not, this ready supply of oxygen and access to the environment might be a problem. This seems to be a major safety trade-off.

We are not prepared at the present time to accept these approaches to defense in depth as being completely adequate. Further, we are not prepared at this time to accept the arguments that increased prevention of core melt or increased retention capacity of the fuel provide adequate defense in depth to justify the elimination of the need for conventional containment structures. This is not to say that we could not decide otherwise in the future, in response to an unusually persuasive argument.

EMERGENCY PLANNING

We agree with the present approach of the staff's proposal. However, we believe that emergency planning should be reexamined in an effort to describe an approach that would be applicable to all types of reactors.

ADDITIONAL ISSUES

How safe should these plants be?

We believe the debate about how safe is safe enough is concluded. The safety goal policy is in place. That should stand as the definition of how safe these advanced reactors, as well as future LWRs, should be. There are, of course, matters of interpretation and implementation with regard to safety goal policy. These need to be dealt with for all types of reactor plant designs. The focus of licensing and regulation for advanced reactors should be consistent with the safety goal policy; no more, no less, no enhancements, no compromises.

The Advanced Reactor Policy states that advanced reactors must be at least as safe as the current generation of LWRs. The staff interprets this to mean the "evolutionary" generation of LWRs now being reviewed by the NRC for preliminary design certification.

We believe the Advanced Reactor Policy requires no more than, and should require no more than, the level of safety called for in the safety goal policy. Reactor developers, i.e., DOE and the industry, may seek a design that is safer than the safety goal would suggest as necessary, or whose safety is more readily apparent to the public. Those are not unreasonable goals for a developer in seeking public acceptance or more economic operation. However, it seems to us inappropriate for the NRC to ratchet on the standard of safety it has established as necessary and sufficient.

To what extent should regulatory requirements accommodate public perception?

The draft paper states that the staff has incorporated only technical considerations in the development of its proposed positions. In particular, they have not attempted to accommodate external factors, such as public perception. We applaud this restraint. And we counsel the Commission to keep safety regulations unambiguously related to protection of the public health and safety.

Extra capacity in decay heat removal and scram systems

The three DOE designs provide much more capacity in decay heat removal and scram systems than are provided in present LWRs. While these important systems in LWRs must be tolerant of single failures, the advanced reactors go well beyond that. The reason for this is the intent to build more robustness into the first two layers of defense in depth and thus permit less in the last two layers, containment and emergency planning.

Two independent scram systems are provided in two of the three proposed designs. Each system is somewhat diverse in design and tolerant, within itself, of single failure. All three design proposals have multiple systems for decay heat removal. In addition to being diverse and resistant to single failure, the extra systems have inherent passive attributes. They apparently will function effectively without motive power or operator intervention.

However, a caution is necessary. Experience in operation and analysis has indicated that redundancy, i.e., extra systems or components, is not as powerful in improving reliability as might be expected. Too often the nature of initiating challenges, or of the complex sequence of events in accidents, seems to cause the extra parts of a system to be faulted along with the main system. The diverse and passive nature of the three designs being considered might ameliorate such unwanted interdependency, but further study is warranted. In addition, while the three proposed designs have these positive features, it is not clear that the NRC's proposed requirements would provide assurance that these desirable diverse and passive attributes would be guaranteed.

Need for prototyping

The staff proposes only modest requirements for prototype testing of the advanced reactor designs. Although, they have recently added a proposed requirement that any designs not incorporating a containment must be tested in prototype at a remote site, we question whether this is enough to carry the process to a point at which the NRC would be willing to license an unlimited number of new power plants. For example, the metallic LMR cores are claimed to have very favorable, inherently stable characteristics in responding to possible transients. These characteristics were not well understood a decade ago.

An excellent experimental and analytical program by ANL with the EBR-II reactor at INEL has effectively demonstrated that the EBR-II system does exhibit such inherently stable and predictable behavior. However, it is not yet clear that such characteristics can be assured for the larger and different LMRs to be used in commercial electric power production. We believe that a more and extensive series of prototype tests will be necessary before design certification could be granted.

Use of cost-benefit analysis

The staff paper proposes that prospective licensees should be required to demonstrate through cost-benefit analysis that design features alternative to those being proposed are not warranted. Presumably, the NRC staff would review such analyses and perhaps suggest alternatives. We believe this is an unworkable and unnecessary strategy. The NRC should concentrate its efforts on specifying design requirements that will result in plants that are in conformance with the safety goal. Consideration of alternatives and costs is properly a function of the designer and owner of a plant. The NRC should have enough confidence in its safety goal that it does not feel the need for the proposed approach.

Design for resistance to sabotage

It is often stated that significant protection against sabotage can be inexpensively incorporated into a plant if it is done early in the design process. Unfortunately, this has not been done consistently because the NRC has developed no guidance or requirements specific for plant design features, and there seems to have been no systematic attempt by the industry to fill the resulting vacuum. We believe the NRC can and should develop some guidance for designers of advanced reactors. It is probably unwise and counterproductive to specify highly detailed requirements, as those for present physical security systems, but an attempt should be made to develop some general guidance.

Operation and staffing

Little is said in the staff paper about requirements for operation and staffing of advanced reactors. We find this to be a serious oversight. Experience with LWRs has shown that issues of operation and staffing are probably more important in protecting public health and safety than are issues of design and construction. The designers of the three reactor proposals seem to be claiming that the designs are so inherently stable and error-resistant that the questions of operation and staffing, so important for LWRs, are unimportant for the advanced reactors. And that, in fact, the advanced plants can be operated with only a very small staff. We believe these claims are unproven and that more evidence is required before they can be accepted.

The two major accidents that have been experienced in nuclear power, those at TMI-2 and Chernobyl 4, were caused, in large measure, by human error. These were not simple "operator errors" but instead were caused by deliberate, but wrong, actions. There are some indications that the advanced reactor designs being considered have certain characteristics tending to make them less vulnerable to such maloperation. But, this has not been demonstrated in any systematic way. The traditional methods of PRA are not capable of such analyses; but, we believe a systematic evaluation should be made. There seems little merit in making claims for the improved safety of new reactor designs if they have not been evaluated against the actual causes of the most important reactor accidents in our experience.

Will regulatory criteria evolve?

The Staff proposal provides for a future milestone in the ongoing design-review-licensing process at which the NRC will step back and make sure that the agreements reached early in the process are still valid, given possible new information and understandings. We believe this is wise and necessary, although it does place a potential licensee at some risk. It should be recognized that this milestone activity might have to include the possibility of changes in the actual requirements, as well as interpretations of requirements.

Focus on the most important residual uncertainties

Although the staff paper discusses uncertainties relative to the development of requirements and designs, it should provide a clearer statement of what the staff believes to be the most important of these. This would assist policymakers in making judgments about the designs and requirements and, perhaps, about whether certain avenues of research should be further pursued before or in parallel with licensing.

Additional comments by ACRS Member Carlyle Michelson are presented below.

Sincerely,

Willliam Kerr
Chairman

Additional Comments by ACRS Member Carlyle Michelson

It is not clear to me that the safety goal in its present form was intended to apply to advanced reactors which do not have conventional containment systems. The guidelines for regulatory implementation might have been different if the Commission had considered that the defense-in-depth approach might not include a containment system on future plants.

It would be unfortunate if the frequency of large release criterion suggested in the present guidelines is used as a basis for justifying the omission of a containment system for an advanced reactor plant at a time when advanced LWRs which might be able to meet the same criterion are required to have containments.

References:

1. Draft Commission Paper from Victor Stello, Jr., for the Commissioners, Subject: Key licensing issues associated with DOE sponsored advanced reactor designs, dated February 9, 1988
2. U.S. Nuclear Regulatory Commission, NUREG-1226, "Development and Utilization of the NRC Policy Statement on the Regulation of Advanced Nuclear Power Plants," published June 1988

→