EM 801-4
NORBERG

TENNESSEE VALLEY AUTHORITY

CHATTANOOGA, TENNESSEE 37401

500C Chestnut Street Tower II

JUN 20 1979

DOCKET NUMBER
PROPOSED RULE PR-Misc. Notice
Reg. Guide

Secretary of the Commission
U.S. Nuclear Regulatory Commission
Washington, DC 20555

Attention: Docketing and Service Branch

Dear Sir:

In accordance with provisions for public review and comment indicated in the Federal Register on June 12, 1974, the Tennessee Valley Authority (TVA) is pleased to provide the enclosed comments on the following regulatory guide:

Regulatory Guide 1.139 - "Guidance for Residual Heat Removal"

Since the content and interpretation of regulatory guides have a large impact on TVA's extensive nuclear commitment, we welcome the opportunity for review and comment. TVA comments on additional regulatory guides will be forthcoming as part of a continuing program.

Very truly yours,

J E Gilleland

J. E. Gilleland
Assistant Manager of Power

Enclosure
cc (Enclosure):

Executive Secretary
Advisory Committee on Reactor Safeguards
U.S. Nuclear Regulatory Commission
1717 H Street, NW.
Washington, DC 20555

Mr. Fred Stetson
AIF, Inc.
7101 Wisconsin Avenue
Washington, DC 20555

Acknowledged by card....ah 7/2

1046 048

7909270 314

ENCLOSURE

TVA's COMMENTS ON REGULATORY GUIDE 1.139

"GUIDANCE FOR RESIDUAL HEAT REMOVAL"

Even before the incident at Three Mile Island, we agreed with the general intent of this regulatory guide and concurred that as a design basis, nuclear power plants should have the capability of reaching cold shutdown from normal operating conditions after any event using only safety grade systems. Further, we believe that this topic needs to be addressed and represents a much more realistic safety concern than a number of other current safety review subjects as anticipated Transients Without Scram. It is not totally clear, however, for what events this regulatory guide applies. It should be clarified as to whether it is applicable only to the events addressed by Chapter 15 of the Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants, or is intended to cover these events plus other events such as fires, non-Chapter 15 pipe failures, etc.

Even if the above clarification is that the guide applies only to non-Chapter 15 events, it is our opinion, based on our present experience and design knowledge, that modifications which would result from the implementation of this guide should be accommodated fairly easily into new plant designs without excessive costs. Our opinion on the incorporation of modifications into operating plants or plants well into the construction or procurement stages is noted later in our specific comments. We would like to point out that over the past several years, we have attempted to provide many of the elements of this regulatory position into our ongoing plants; however, the full degree of rigor that is called for by this guide was not used.

For ease of identification, our comments are addressed to the positions noted in Part C of this regulatory guide but they are applicable to corresponding areas in the remaining portions of this guide.

1. Section C.1.a

   We agree with C.1.2 but we believe the term "cold shutdown" needs to be defined to eliminate confusion, as in the Standard Review Plan Branch Technical Position RSB5-1 Rev. 1 which contains a clarifying definition.

1046 042

2. Section C.1.b

We agree that it is desirable that systems needed to reach cold shutdown be designed to accomplish their function assuming single failures. However, we believe that allowing operator action outside the main control room (MCR) only after a single failure, when combined with the safety-grade equipment requirements of position C.1.a and the loss-of-power conditions of C.1.b. does not seem to have a logical basis, is unduly restrictive, and places undue economic penalties on plant control design for little, if any, increased safety margin. As an illustration of this concern, consider the case of meeting Branch Technical Position (BTP) EICSB-18 versus technical specification cooldown rates and pressure limitations. To reach cold shutdown in a manner that does not present a safety problem but which could possibly lead to a violation of the conservatively set technical specification cooldown rates and pressure limits, the operator may need to manipulate some valves (such as residual heat removal (RHR) throttle valves and safety injection tank isolation valves). However, to meet the requirements of BTP EICSB-18, power to these valves has been removed by local removal of breakers. Thus, before the operator can gain control of the valves, action outside of the MCR is necessary to reinsert these breakers. Requiring such defeat operations to be controllable from the MCR would necessitate considerable unwarranted and uneconomic redesign of control systems including MCR panels while gaining little, if any, increased safety margin. In fact, adding such additional equipment may actually degrade the overall system by making it less reliable.

We believe that a better design philosophy is that:

a. Remote control of those systems necessary to reach cold shutdown must be provided within the MCR, but

b. These systems and controls can use normal power supplies and be non-redundant, non-safety-grade if:

   (1) Emergency powered, redundant safety-grade backup systems are provided; and

   (2) All necessary controls for these safety-grade systems are located in close proximity to the MCR and separated from any possibly contaminated fluid system areas (that is, for example, within the Control Building and not within the Auxiliary

1046 050

Building or not just outside a major pump room), while meeting all operator protection and operator time limitations (e.g., those given in ANS draft standard N660).

By meeting these two item b provisions, operator action outside the MCR should be permissible for the majority of initiating events, single failures, and power source failures. The provisions also help address the problems associated with designing two train essential systems to be able to cope with initiating events that affect one train and single failures in the opposite train. It may still be necessary, unfortunately, to exclude some dual-purpose two-train systems from the single failure design requirements if other than Chapter 15 events are to be included within the scope of this regulatory guide. Such exclusions need to be noted.

Overall though, we believe that this approach results in a design which is safe, efficient, effective, and provides margin for unknowns. Therefore, we recommend that C.1.b, in conjunction with C.1.a, should be modified to permit use of this design approach.

3. Section C.1.c

We believe the "36 hour" time limit requirement is arbitrary and has no technical basis. In order to permit some reasonable deviation from this requirement, we recommend the following rewording " . . . a cold shutdown condition be achieved within a reasonable time after shutdown (an adequate design objective is 36 hours)." This would more clearly allow for minor deviations, such as being able to achieve cold shutdown in 40 hours, without causing undue effort on the part of the applicant or the staff. Also, as in comment 1 above, the term "cold-shutdown" needs to be defined so that the applicant may clearly know what the design requirements are.

4. Section C.2.a

We believe some clarifications or modifications to this section are needed because several conflicting functional requirements have been imposed on the residual heat removal (RHR) system suction isolation valves. These requirements, which must be accomplished in a single failure proof manner, are:

a. Protect the RHR system from overpressurization transients within the reactor coolant system (RCS), i.e., close when required

b. Provide the capability to get on RHR cooling so that cold shutdown may be attained, i.e., open when required

c. Isolate the RCS after a pipe failure in the RHR system while on RHR cooling, i.e., close when required

d. In some designs, protect the RCS from low temperature overpressurization transients by relief valves in the RHR downstream of the RCS and RHR isolation valves, i.e., remain open when required

e. Prevent damage to the RHR pumps from intentional or spurious closure of the RHR isolation valves, i.e., remain open when required or provide net positive suction head (NPSH) protection for the RHR pumps.

In the past, the NRC has addressed through various documents only one or two of these requirements, e.g., see Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants, Revision 0, item 6.3.2 (16), Revision 1, item 6.3.2.16, and Regulatory Guide (RG) 1.70 Revision 2, item 6.3.2.2. This partial approach has created some problems. For example, the requirement for automatic isolation valve closure on high RCS pressure (to meet function a, is required in revisions 0, 1, and 2 of the SAR guide and is implied in item C.2.a of RG 1.139) has created situations where a single active failure could close at least one valve in each suction line of a normal two-train RHR system. This closure is a violation of functions d and e. Thus, consideration of all of the functions placed on these valves needs to be given when determining regulatory positions.

In this case, we believe that the best method to treat all of these conflicting requirements is to use a combination of passive relief devices, four-channel actuation, and remotely operable isolation valves. The passive relief devices are to be utilized to meet functions a and d while the four-channel actuation and remote operability are to meet functions b, c, and e in addition to helping meet single failure rules for a and d. These methods, in turn, eliminate the need for automatic valve closure and its potential for causing undesirable pump damage. In addition, the diversity in pressure sensors to be used in valve interlocks may not be necessary if the passive relief devices are relied on for the main overpressurization protection with the backup being remote operability of the valves.

We believe utilization of these methods will eliminate the present confusion blanketing the RHR isolation valve functional requirements while yielding a truly safe design. Therefore, we recommend that C.2.a be modified to permit and recognize these design methods.

5. <u>Section C.2.b and C.3.a</u>

See comment 4 above concerning use of relief valves and automatic isolation capability.

6. <u>Section C.4</u>

This section implies that automatic protection against conditions such as thermal overheating and low NPSH should be included in any RHR system design for any operating mode including emergency core cooling. This appears to be in direct conflict with other NRC requirements that do not permit automatic equipment protection to be employed on equipment used for accident mitigation (see RG 1.106 and BTP EICSB-17). We do not believe that bypasses of this protection should be employed in this case.

7. <u>Section C.5</u>

We are concerned that in order to meet these testing requirements, detailed measurements for both core hot spots (implied from position B.2.a) and boron mixing would be imposed. Such detailed measurements are very impractical and would be extremely costly. We recommend that this section be modified to state that gross measurements, in combination with supporting calculation, are acceptable methods to meet these requirements.

8. <u>Section C.6</u>

The "4 hours" time limit appears arbitrary and, therefore the discussion in comment 3 concerning the "36 hour" time limit applies. Also, although not specifically stated here in C.6, it can be implied from discussion B.2.a that the seismic category I cooling water source must be of secondary side (e.g., condensate) or better quality. We believe that such a requirement is unnecessary. Our design philosophy is that the auxiliary feedwater sources should be of such a seismic qualification and a water quality that, for the conditions and duration of operation, their use will not result in degradation of steam generator tube integrity to an unsafe extent or that the minimum safe steam generator heat transfer capacity is lost.

(Note: Such a philophy is consistent with that in Draft 5 of ANSI Standard N667 on Auxiliary Feedwater System for Pressurized Water Reactor). This concept permits the use of a primary AFW source which does not meet safety grade, seismic and secondary side quality requirements. As a backup source, for those very low probability events when the preferred AFW source is not available, such a philosophy does require a safety grade, seismically qualified AFW supply but it does not require that this source be of a secondary side quality. We believe this philosophy yields the most economical AFW supply design while maintaining a fully adequate safety margin. We, therefore, recommend that both B.2.a and C.6 be modified to clearly permit this design philosophy.

9. Section C.7

As stated in comment 1 above, "cold shutdown" needs to be defined. Also, it could be interpreted from position C.6 that these operational procedure requirements need be taken only to the RHR system initiation. We believe such procedures need to be defined beyond just RHR initiation to full cold shutdown conditions. We, therefore, suggest appropriate modifications be made to C.7 to clearly define the time span to be considered when addressing the C.7 requirements.

10. Section D

We agree with the intent of this guide but believe full implementation of its requirements on plants either in operation or for which a major portion of the equipment has been purchased is not warranted unless major safety flaws (such as equipment environmental qualification discrepancies) are discovered during the review process. While regulatory guides are not supposed to be true "requirements," the issuance of such a guide tends to channelize staff thinking and places the burden of proof on the adequacy of a plant design which deviates from any guide on the applicant. For the plants noted, it is our opinion that the design bases and philosophy employed for them does provide adequate assurance that the health and safety of the public is preserved and that any major effort required to justify these designs when compared to this regulatory guide is not necessary and would be a misdirected effort. The case-by-case review of these plants as called for by this regulatory guide position could indeed lead to such an effort and probably some degree of backfitting on most plants. Although this would increase the plant's margin of safety, the additional margin, unless major safety flaws are found, is not sufficient to justify any large scale evaluation and backfitting effort.