DATE ISSUED:

ACRS-1821

MINUTES
SAFETY PHILOSOPHY, TECHNOLOGY, AND CRITERIA
SUBCOMMITTEE MEETING
JAN 28, 1981
LOS ANGELES, CALIF

The ACRS Subcommittee on Safety Philosophy, Technology and Criteria held a meeting on January 28, 1981 at the Best Western Airport Park Hotel, 600 Avenue of Champions, Inglewood, California. The purpose of this meeting was to discuss the views that Subcommittee members had as to the requirements for new (beyond NTCP) plants in preparation in responding to Commissioner Ahearne's request for ACRS comments on this subject. Notice of this meeting was published in the Federal Register of January 15, 1981. A copy of the notice is included as Attachment A. A list of the attendees is included as Attachment B. A schedule for this meeting is included as Attachment C. The handouts for this meeting are included as Attachment D. No written statements or requests for time to make oral statements were received from members of the public. The meeting was attended by D. Okrent, Chairman; M. Bender, J. C. Mark, C. P. Siess, and D. Ward (Subcommittee members); and H. Etherington, Subcommittee consultant and R. Savio of the ACRS Staff. Dr. Savio was the Designated Federal Employee for the meeting. The meeting was opened at 1:00 pm on January 28, 1981 with a short presentation given by Dr. Okrent summarizing the schedule and the goals for the day's meeting. The discussions were adjourned at 5:30 pm on the same day. The entire meeting was held in open executive session.

EXECUTIVE SESSION

A number of ways of developing improved requirements were briefly discussed by the Subcommittee. These were:

(a) A reexamination of the hardware/procedure modifications which were implemented as a result of the TMI-2 accident review and to evaluate their effectiveness and the potential for developing more generic requirements from this experience.

(b) The use of probabilistic analysis as a basis for defining plant systems important to safety and developing design requirements.

(c) A review of the General Design Criteria as to their adequacy and their implementation in the Regulatory Guides and Branch Technical Position.

(d) A review of the adequacy of the requirements for DHR systems in the U.S. and foreign countries and the basis for these requirements.

(e) The establishment of criteria dealing with sabotage and the evaluation of overall (in the sense of overall safety, effectiveness as separations and controlled access).

The ACRS Staff (M. Libarkin, G. Quittschreiber, and J. C. McKinley) prepared a paper on proposed revisions to the GDCs dealing with decay heat removal, the single-failure criteria, and the treatment of common-mode failure. This paper is attached. The Subcommittee was in general agreement with the approaches suggested and felt that they merited further discussion and investigations. The design philosophy associated with the German DHR systems was discussed. The designs generally utilize a high degree of redundancy and a bunkered train. It was suggested that the basis by which these designs were developed needed to be explored further by the Subcommittee.

The treatment of Class 9 accident scenarios was discussed. It was suggested that realistic core melt source terms should be used in this type of evaluation and that the necessary information should be developed. It was also suggested that an improved treatment of the hydrogen release hazard also needs to be developed and that the specific site characteristics need to be understood and considered.

Quantitative safety goals were discussed. It was proposed that the quantitative goals need to be established for the systems which prevent core melt. It was noted that it is very difficult to demonstrate either by analysis or by experiment thatindividual systems have a very low ($<10^{-3}$/yr to 10^{-4}/yr) unavailability. Safety goals which require a lower unavailability would require the use of redundant/diverse systems and careful attention to avoiding common failure modes. The adequacy of the single failure criteria was discussed. It was noted that the criterion is inadequate in itself when applied to systems with a high unavailability. In addition, consideration of common mode failure is necessary. Highly reliable performance is to be achieved with redundant/diverse systems.

The schedule for responding to Chairman Ahearne's requirements for new plants was discussed. It was agreed to attempt to have issued a response in July 1981. It is expected that another meeting on this subject will be held in about two months. A list of action items generated at this Subcommittee meeting is included as Attachment E.

Dated: January 12, 1981.
John C. Hoyle,
Advisory Committee Management Officer.
[FR Doc. 81-1408 Filed 1-14-81; 8:45 am]
BILLING CODE 7590-01-M

Advisory Committee on Reactor Safeguards, Subcommittee on Fort St. Vrain; Meeting

The ACRS Subcommittee on Fort St. Vrain will hold a meeting on January 27, 1981 at the Fort St. Vrain Visitors Center, 16805 Road 19½, Platteville, CO (near Longmont, CO). The Subcommittee will review operating experience, degree of success in eliminating the core power fluctuations, plans for testing and operation above 70% of rated power, core performance (fuel and structural), and plans for future operations, modifications, refueling, and shift manning requirements. Notice of this meeting was published December 22, 1980.

In accordance with the procedures outlined in the **Federal Register** on October 7, 1980, (45 FR 66535), oral or written statements may be presented by members of the public, recordings will be permitted only during those portions of the meeting when a transcript is being kept, and questions may be asked only by members of the Subcommittee, its consultants, and Staff. Persons desiring to make oral statements should notify the Designated Federal Employee as far in advance as practicable so that appropriate arrangements can be made to allow the necessary time during the meeting for such statements.

The entire meeting will be open to public attendance.

The agenda for subject meeting shall be as follows:

Tuesday, January 27, 1981
8:30 a.m. until the conclusion of business

During the initial portion of the meeting, the Subcommittee, along with any of its consultants who may be present, will exchange preliminary views regarding matters to be considered during the balance of the meeting.

The Subcommittee will then hear presentations by and hold discussions with representatives of the NRC Staff, their consultants, and other interested persons regarding this review.

Further information regarding topics to be discussed, whether the meeting has been cancelled or rescheduled, the Chairman's ruling on requests for the opportunity to present oral statements and the time allotted therefor can be obtained by a prepaid telephone call to the cognizant Designated Federal Employee, Mr. John C. McKinley (telephone 202/634-3267) between 8:15 a.m. and 5:00 p.m., EST.

Dated: January 12, 1981.
John C. Hoyle,
Advisory Committee Management Officer.
[FR Doc. 81-1410 Filed 1-14-81; 8:45 am]
BILLING CODE 7590-01-M

Advisory Committee on Reactor Safeguards, Subcommittee on Safety Philosophy, Technology and Criteria; Meeting

The ACRS Subcommittee on Safety Philosophy, Technology and Criteria will hold a meeting at 1:00 p.m. on January 28, 1981 at the Best Western Airport Park Hotel, 600 Avenue of Champions, Inglewood, CA 90301. The Subcommittee will discuss requirements for new (beyond Near-Term Construction Permit) reactor plants.

In accordance with the procedures outlined in the **Federal Register** on October 7, 1980 (45 FR 66535), oral or written statements may be presented by members of the public, recordings will be permitted only during those portions of the meeting when a transcript is being kept, and questions may be asked only by members of the Subcommittee, its consultants, and staff. Persons desiring to make oral statements should notify the Designated Federal Employee as far in advance as practicable so that appropriate arrangements can be made to allow the necessary time during the meeting for such statements.

The entire meeting will be open to public attendance except for those sessions during which the Subcommittee finds it necessary to discuss predecisional information. One or more closed sessions may be necessary to discuss such information. (SUNSHINE ACT EXEMPTION (9)(B)). To the extent practicable, these closed sessions will be held so as to minimize inconvenience to members of the public in attendance.

The agenda for subject meeting shall be as follows:

Wednesday, January 28, 1981
1:00 p.m. until the conclusion of business

During the initial portion of the meeting, the Subcommittee, along with any of its consultants who may be present, will exchange preliminary views regarding matters to be considered during the balance of the meeting.

The Subcommittee will then hear presentations by and hold discussions with representatives of the NRC Staff, their consultants, and other interested persons regarding this review.

Further information regarding topics to be discussed, whether the meeting has been cancelled or rescheduled, the Chairman's ruling on requests for the opportunity to present oral statements and the time allotted therefor can be obtained by a prepaid telephone call to the cognizant Designated Federal Employee, Mr. Richard Savio (telephone 202/634-3267) between 8:15 a.m. and 5:00 p.m., EST.

I have determined, in accordance with Subsection 10(d) of the Federal Advisory Committee Act, that it may be necessary to close some portions of this meeting. The authority for such closure is Exemption (9)(B) to the Sunshine Act, 5 U.S.C. 552b(c)(9)(B).

Dated: January 12, 1981.
John C. Hoyle,
Advisory Committee Management Officer.
[FR Doc. 81-1409 Filed 1-14-81; 8:45 am]
BILLING CODE 7590-01-M

Advisory Committee on Reactor Safeguards, Subcommittee on San Onofre Units 2 and 3; Meeting

The ACRS Subcommittee on San Onofre Units 2 and 3 will hold a meeting on January 31, 1981 at the Best Western Airport Park Hotel, 600 Ave. of Champions, Ingelwood, CA 90301. The Subcommittee will meet with representatives of the Southern California Edison Company and the NRC Staff to review the seismology and geology related items for San Onofre Units 2 and 3 for an Operating License.

In accordance with the procedures outlined in the **Federal Register** on October 7, 1980, (45 FR 66535), oral or written statements may be presented by members of the public, recordings will be permitted only during those portions of the meeting when a transcript is being kept, and questions may be asked only by members of the Subcommittee, its consultants, and Staff. Persons desiring to make oral statements should notify the Designated Federal Employee as far in advance as practicable so that appropriate arrangements can be made to allow the necessary time during the meeting for such statements.

The entire meeting will be open to public attendance.

The agenda for subject meeting shall be as follows:

Saturday, January 31, 1981
8:30 a.m. until the conclusion of business

During the initial portion of the meeting, the Subcommittee, along with any of its consultants who may be present, will exchange preliminary views regarding matters to be considered during the balance of the meeting.

The Subcommittee will then hear presentions by and hold discussions

attach A

TIME 1:00 pm

DATE 28 jan

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

MEETING Safety Philosophy, Technology & Criteria

ATTENDEES PLEASE SIGN BELOW

(PLEASE PRINT) NAME	BADGE NO.	AFFILIATION
1 [illegible]		
2 H. E. [illegible]		
3 [illegible]		
4 J. C. [illegible]		
5 M. [illegible]		
6 [illegible]		
7 [illegible]		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		

Attach B

SCHEDULE FOR JANUARY 28, 1981
SUBCOMMITTEE
SAFETY PHILOSOPHY, TECHNOLOGY, AND CRTIERIA

EXECUTIVE SESSION 1:00 until COB

Attach C

UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, D. C. 20555

January 26, 1981

MEMORANDUM FOR: David Okrent, ACRS

FROM: M. W. Libarkin, Assistant Executive Director for Project Review

SUBJECT: PROPOSED REWRITTEN GENERAL DESIGN CRITERIA

As you requested, John McKinley, Gary Quittschreiber, and I have been considering possible modifications to selected general design criteria. We have focussed on those relating to decay heat removal and the single failure criterion initially. The enclosed suggestions are dual in nature: first, an approach which has had the benefit of somewhat broadened and more detailed consideration and which, we believe, is therefore more likely to be translatable into practical designs; second, an approach intended to go beyond that and address specific difficulties which have arisen in the course of Committee discussion, etc. As a result, we have included two decay-heat-removal-related concepts. One is largely, "lifted" from recent German design criteria aimed at insuring the continued ability to remove decay heat; the second goes beyond that to address the subject from the standpoint that the secondary system may not be available. Similarly, the single failure criterion has been approached using an assumption that protection systems enjoy a higher functional reliability than other systems important to safety and that a general requirement for criteria, across the board, analagous to those which have been established for protection systems would be an improvement.* The second approach recognizes the questions which have been raised about current LWR protection systems (e.g., the use of untestable scram relays, etc.) and includes an attempt to describe all of the characteristics of common-mode failure and to write criteria which would preclude those which are design-related.

*WASH 1400 and more recent ATWS related studies gave RPS failure probabilities in the range 10^{-5} to 10^{-4}; WASH 1400 also gave failure probabilities for important hydraulic systems on the order of 10^{-3}.

Attach: 0

BACK-UP RESIDUAL HEAT REMOVAL

Discussion

It has been frequently mentioned during ACRS meetings that significant improvements could and should be made in the capability of U.S. nuclear power reactors to remove the residual heat following a scram and the loss of the normal heat sinks.

The Committee has expressed its concern that some of the residual heat removal (RHR) systems are of low pressure design and must be reliably isolated from the primary system until that system can be depressurized (Generic Items No. 48 - Isolation of Low Pressure from High Pressure Systems).

Example has also been made of the German "bunkered system" as a feature that should be added to U.S. reactors.

A study at UCLA by J. C. Ebersole and D. Okrent proposed "An Integrated Safe-Shutdown Heat Removal System for Light Water Reactors" (UCLA - Eng - 7651, May 1976).

The current requirements for RHR are contained in General Design Criterion No. 34.

> ***Criterion 34—Residual heat removal.*** A system to remove residual heat shall be provided. The system safety function shall be to transfer fission product decay heat and other residual heat from the reactor core at a rate such that specified acceptable fuel design limits and the design conditions of the reactor coolant pressure boundary are not exceeded.
>
> Suitable redundancy in components and features, and suitable interconnections, leak detection, and isolation capabilities shall be provided to assure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming onsite power is not available) the system safety function can be accomplished, assuming a single failure.

The German RHR requirements are set out in the RSK Guidelines with the requirements for Emergency Core Cooling.

"22. Systems for Post-Incident Heat Removal

"22.1 Emergency Core Cooling and Residual Heat Removal System

(1) A reliable ad efficient redundant emergency core cooling and residual heat removal system shall be available for the removal of heat after loss-of-coolant accidents. The system shall be capable of keeping core temperatures at long-term low values in case of an occurrence of leaks and breaks in the pressure-retaining boundary as specified in Sec. 21.1...."

"22.2 Emergency System

(1) In case the control room is not in a functionable state it shall be assured that the emergency system will bring the plant into a safe state without any manual intervention and that the plant can remain in this state for at least 10 hours. In addition, it shall be possible, with the aid of the emergency system by a blowdown on the secondary side, to bring the plant into a state which will permit the subsequent residual heat removal through the special emergency heat removal system. No redundancy is required for this emergency heat removal system."*

"Emergency measures need not be automated if there is sufficient time available prior to their initiation or if their initiation can be provided for by administrative measures. Local auxiliary measures may be reverted to for the long-term control in an emergency case."

"(2) In detail, the emergency system shall comply with the following safety-related requirements:

1. Components and subsystems of the emergency system shall be protected against external events and events caused by third parties.

*Emphasis added

2. A consistent separation of the emergency system from other nuclear power plant systems shall prevent the function of the emergency system from being unacceptably affected by damage caused in plant areas which may be destroyed. This applies not only to process systems but also to energy supply systems and the reactor protection system.

3. In addition, the separation shall assure that unauthorized interventions or maloperations in the control room or in other plant areas which are not especially protected cannot lead to any unacceptable impairment of the function of the emergency system.

4. Any intervention in the emergency system, be it for operational reasons or testing purposes, shall be prohibited if such intervention cannot be made undone or completed in case of an emergency and will lead to an unacceptable impairment of the function of the system."

Proposal

In order to provide an additional means of removing residual heat in U.S. reactors an additional design criterion is proposed as follows:

"34.a.1 A backup residual heat removal system shall be provided. This system shall be designed to transfer fission product decay heat and other residual heat from the reactor core at a rate such that specified acceptable fuel design limits and design conditions of the reactor coolant boundary are not exceeded. The system shall be capable of operation over the full range of primary system temperature and pressure. It shall keep the reactor core within specified limits for at least n* hours without replenishment of consumable materials (fuel, water lubricants, etc.) and there shall be sufficient consumable material on site for at least seven days of continuous operation."

*n = 10 hours in the German guidelines.

The above performance requirements are within the current design capability since all German reactors have such a capability. If it is desired to make the backup system more reliable than the German practice, a second part of the criterion would be:

"34.a.2 The backup residual heat removal system will be dedicated to this purpose only and shall have its own power supply and be independent of all other plant systems. It shall be protected against impacts from both externally and internally generated missiles as well as from the effects of crashing aircraft. The backup system shall be spacially and systemically separated from other heat removal systems so that no single credible event could incapacitate all systems. It shall have such redundancy in components and features, and suitable interconnections, leak detection and isolation capabilities to assure that the system's function can be accomplished assuming a single failure of passive or active components and multiple active component failures for those credible events where common mode failure could result from adverse environmental conditions, extreme plant conditions, or maintenance errors of a generic nature."

This reliability requirement attempts to incorporate the German requirements and add redundancy and common mode failure protection. It is an attempt to improve on the U.S. single failure criterion. No system has yet been designed to such requirements.

Since the proposed system is safety grade it should have QA, inspection, and testability, therefore a third part of the criterion would be:

"34.a.3 The backup residual heat removal system shall have components and shall be arranged in such a way as to meet the standards of design, quality and testability for systems important to safety."

This quality assurance and testability requirement is the same as for current systems that are important to safety.

Supplemental Thoughts

In addition, it has been suggested by at least one ACRS member (J. C. Ebersole) that nuclear power plants should have the capability to achieve the cold shutdown condition using only safety grade equipment and that one such method would be a bleed-and-feed capability on the primary system.

If it is desired that the backup system be independent of the PWR steam generators then another high pressure heat transfer system would be required.

To accomplish this, the criterion could be phrased as follows:

"A backup residual heat removal system shall be provided that is independent of the secondary system. This system shall be designed to transfer fission product decay heat and ...."

The above proposals are tentative and no attempt has been made to analyze costs, practicability, or risk reduction. The proposal is aimed at providing a residual heat removal system that is capable of reliably operating over the full range of reactor conditions, be independent of other secondary systems, and be protected from adverse external influences.

SUPPLEMENT TO SINGLE FAILURE CRITERION

10 CFR 50 Appendix A states "Multiple failures resulting from a single occurrence are considered to be a single failure." Criteria 17, 34, 35, 38, 41, and 44 require that the system safety function can be accomplished assuming a single failure; therefore, the existing General Design Criteria do require consideration of the Common Cause/Common Mode (CC/CM) failures; however, no systematic approach has been used to ensure that multiple failures resulting from a single occurrence are adequately covered, especially with regard to fire, flood, earthquake, and human error occurrences.

The General Design Criteria do expand on the Single failure criteria for reactor protection systems in Criterion 21 and 22, and provide a specific approach to ensure that multiple failures do not result from single, initiating failures.

Reactor Protection Systems in nuclear plants are designed to more stringent criteria than other nuclear systems in present day plants and are probably the less susceptible to loss of safety function due to CC/CM failures. The special requirements for protection systems in Criteria 21 and 22 could be applied to other safety systems.

The present single failure wording in Criteria 17, 34, 35, 38, 41, and 44 could be modified to assure that randomness of failure of redundant systems is not breached by the influence of interactions of other systems or by interactions from the same system using the requirements for protection systems in Criteria 21 and 22. The principal difference resulting from

such a change is that at least three trains for each safety system would likely be needed in order to allow one train to be out of service for testing, maintenance, or repair.

Modify Criteria 17, 34, 35, 38, 41, and 44 as follows:

The system shall be designed for high functional reliability and inservice testability commensurate with the safety functions to be performed. Redundancy and independence designed into the system shall be sufficient to ensure that (1) no single failure results in loss of the system function and (2) removal from service of any component, train, or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the system can be otherwise demonstrated.

The system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant trains or channels do not result in loss of the system function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques such as physical separation, barrier protection, functional diversity or diversity in component design, and principles of operation, shall be used to the extend practical to prevent loss of the system function.

PROBABILISTIC ASSESSMENT CRITERIA

Professor Birkhofer, RSK, said in a paper IAEA-CN-30/6.5 given at the Stockholm 20-24, 1980 IAEA Meeting -

"The 'Safety Criteria' of the Federal Minister of the Interior demand: 'In order to verify the well-balancedness of the safety concept, and to supplement the deterministic methods of safety assessment of reactors, the reliability of safety-related systems and main components should be evaluated using probabilistic methods as far as this is possible according to the state of the art with sufficient accuracy'".

The Single Failure Criteria could be supplemented with the following probabilistic assessment criteria to demonstrate the acceptability of the overall system design by requiring the following:

The deterministic safety design criteria should be supplemented on safety-related portions of the plant using "state-of-the-art" probabilistic assessment methods. Weak points of system design should be detected and corrected as practical. Relative probabilistic assessment should be used to decide on system options, to optimize maintenance procedures, and to determine appropriate maximum allowable repair times in redundant systems.

Since there have been questions raised about the adequacy of RPS designs (e.g., as ATWS initiators in connection with the testability of scram relays, etc.), a different approach may be thought more desirable.

Discussion

A widespread perception has been evidenced recently within the ACRS and among others that the single failure criterion does not assure adequate functional reliability, and that multiple failures must be considered. For purposes of this discussion, it will be assumed that what is intended is the consideration in design of common-mode failures of components or systems, and not simultaneous

or sequential, multiple random failures.

It is proposed to retain the single failure criterion where it now appears in the G.D.C., but to augment it by requiring the affected system designs to accommodate those common-cause failure mechanisms which are amenable to mitigation by design approaches.

WASH-1400, in a discussion of the treatment of common-mode failure, provided listings of classes of potential common-mode mechanisms and so-called Component Combination Properties which would indicate susceptibility to such failures. It is proposed to use these as an initial framework within which to consider the subject. (Not all types of common-cause failure mechanisms are included. An obvious omission is <u>deliberate</u> human intervention: sabotage).

<u>TABLE 1</u>

<u>Classes of Potential Common-Mode Mechanisms</u>

A. Design defects

B. Fabrication, Manufacturing and Quality Control[1/] Variations

C. Test, Maintenance, and Repair Errors

D. Human Errors

E. Environmental Variations (Contamination, Temperature, etc.)[2/]

F. Failure or Degradation Due to an Initiating Failure

G. External Initiations of Failure

1/ It is not clear that Q.C. is appropriate since, except in the case of the most egregious mismanagement, it is likely to lead only to a failure to detect a defect and not to the defect itself.

2/ Accident and non-accident

TABLE 2

Component Set Properties Indicating Potential Common-Cause Susceptibility

1. All components identical in type and specification (A,B)[1/]
2. Components all under the same maintenance or test (C)
3. All components having similar failure sensitivity (E,G)
4. Components all in the same locations (E,F,G)
5. Components all exposed to a possible accident environment (E)
6. All components loaded or degraded by a previous failure (F)
7. All component failures human-initiated (D)

Examples of Modified G.D.C.

A design criterion incorporating the single failure criterion was chosen as an example of how common cause failure modes could be recognized as contributors to functional unreliability in modifying the G.D.C. The added language would be incorporated wherever in the G.D.C. the single failure criterion was invoked.

1. Criterion 44-Cooling Water

"A system to transfer heat from structures, systems, and components important to safety, to an ultimate heat sink, shall be provided. The system safety function shall be to transfer the combined heat load... under normal operating and accident conditions.

Suitable redundancy in components and features, and suitable interconnections, leak detection, and isolation capabilities shall be provided to assure that...the system safety function can be accomplished, assuming a single failure."

In addition, components comprising this system, and which are considered part of a redundant set, shall not be identical in type and specification, shall not be located within the same compartment or otherwise in proximity to one another, shall be designed or located such that failures leading to possible damaging influences such as heat or water do not commonly affect all of any redundant component set, and shall be so designed or arranged that any postulated mechanical or electrical failure of interconnected equipment does not commonly affect all of any redundant component set. In connection with the last requirement, excesses in whatever service (e.g., voltage, frequency, flow, pressure, temperature, etc.) is provided or controlled by the system including the failed component should be considered, as well as "on-off" failures.

The proposed additonal requirements are aimed at precluding classes A, B, E, F, and G of the potential common-mode mechanisms listed in Table 1. Some of the defining language was taken from the Committee's October 1979 report on the IP-3 systems interaction study.

As it stands, the added requirements were produced simply by using phrases intended to preclude the properties in Table 2 associated with those mechanisms (A,B,E,F,G) which are considered amenable to mitigation by design approaches. However, some of these have been the source of some controversy in the past, and perhaps that should be recognized. In particular: the requirement for diversity has been attacked on the grounds that, if a clearly superior design

for a piece of equipment can be identified, it should be used; the requirement for compartmentalization has been attacked on the grounds that it makes access, inspection, etc. more difficult. If it seems desirable to recognize these objections, the addition could be modified:

> "In addition, components comprising this system, and which are considered part of a redundant set, shall not be identical in type and specification, 1/ shall be located with adequate separation or protection to prevent failures in nearby systems or in this system from commonly affecting all of any redundant component set, shall be designed or located such that any failures leading to possible damaging influences such as heat or water do not ....."

1/ This requirement is subject to a showing that none of the available component types is clearly superior in reliability to any others available.

Subcommittee Action Items

1. Develop a list of specific examples as to where the Single Failure Criterion proved not to be adequate. The object would be to use these examples to gain insight as to how the Single Failure Criterion could be improved. The existing risk/reliability assessment and the existing review and operating experience would be sources of this information.

2. Develop a list of the GDCs dealing with CMA and a list of the Reg Guides, BTP, etc which are used to implement this aspect of the GDCs.

3. Develop comparative system descriptions of the decay heat removal systems for the current BWR and PWR plants.

4. Schedule a session with the NRC Staff during which the current German DHR design philosophy and DHR designs can be discussed.

5. Schedule a closed sabotage session during which methods of improving the plants resistance to sabotage can be discussed.

6. Schedule sessions during which the fundamental sabotage philosophy can be discussed, i.e., what kinds of sabotage can be prevented and what types of consequences will need to be mitigated.

7. Schedule discussions which deal with the types of sites and site characteristics which are important in a core melt accident and the instances in which filtered vents and core-retention devices will be beneficial. The discussion should address when a core melt into the ground can be dealt would have acceptable consequences and what could be done to mitigate the consequences of such an event. Public acceptance of such an event, even when it does not result in severe radiological consequences, should be considered.

8. Explore with the NRC Staff what could be done in the way of improving existing containment types if the manufacturer was not constrained by an existing design.

ATTACHMENT E