UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

ENCLOSURE 2

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

RELATING TO POSTULATED DC BATTERY POWER SUPPLY FAILURE

AND ECCS REQUIREMENTS

COMMONWEALTH EDISON COMPANY

QUAD CITIES STATION UNITS 1 AND 2

DRESDEN STATION UNITS 2 AND 3

DOCKET NOS. 50-254/265 AND 50-237/249

1.0 INTRODUCTION

By letter dated December 21, 1987 (Ref. 1), Commonwealth Edison Company (CECo), the licensee for the Quad Cities (Units 1 and 2) and Dresden (Units 2 and 3) responded to an informal inquiry from the NRC concerning an event at another plant. This event (to be discussed later) occurred at the Fermi 2 plant and involved the low pressure coolant injection (LPCI) system swing bus design flaw identified as a result of a procedural error (Ref. 2). The Quad Cities and Dresden plants have LPCI Loop Select Logic similar to the Fermi 2 plant and a direct current (DC) battery power supply with a swing bus design. The staff's inquiry also concerned the issue of whether or not CECo's Quad Cities and Dresden plants would be in compliance with the requirements of 10 CFR 50.46 regarding Emergency Core Cooling Systems (ECCS) during the nearly two year period needed to implement on all its affected plants the necessary modifications to correct the design flaw in the (DC) battery power supply swing bus transfer system. This ECCS compliance issue is one subject of this Safety Evaluation Report (SER).

The letter (Ref. 1) did not address the issue of the DC battery swing bus transfer system design flaw or modifications to correct the flaw. Rather, CECo stated in the letter that it had identified one of the analyses for the Quad Cities Unit 1 Cycle 10 reload submittal (Ref. 3) as being in error. CECo stated that the reload submittal incorrectly identified battery failure as the worst single active failure for the postulated design basis Loss of Coolant Accident (LOCA) for Quad Cities Unit 1. CECo stated that the failure of one division of the DC power system would be a passive failure and that it was not part of the Quad Cities Station licensing basis. CECo concluded that the remaining ECCS equipment for the scenario referred to as battery failure, represents the double active failure of both a Diesel Generator (DG) and a high pressure coolant injection (HPCI) system. CECo reported that the maximum peak clad temperature (PCT) for this double active failure event bounds the PCTs for both the DG failure event and the LPCI injection valve failure event which are the limiting single active failure events. These results are presented in the

14

Quad Cities ECCS analysis report (Ref. 4) which was part of the Quad Cities Unit 1 Cycle 10 reload submittal (Ref. 3).

By letter dated December 22, 1987 (Ref. 5), CECo provided additional information on postulated DC battery power supply failures. In this letter, CECo agreed to provide an evaluation of the probability of a postulated DC battery failure coincident with LOCA and Loss of Offsite Power (LOOP). In Attachment 3 to Reference 5, CECo presented information concerning the safety significance of a DC battery failure at its Quad Cities and Dresden plants. CECo concluded (1) that the sequence of events which must occur in a very narrow time window for a coincident LOCA, LOOP and DC battery failure is highly unlikely, (2) that its DC battery power supply system is highly reliable, and (3) that its surveillance and monitoring activities help ensure the high reliability of the battery system. CECo also stated that it would evaluate the existing Quad Cities and Dresden LPCI injection valve swing bus transfer system relative to the recent flaw identified at the Enrico Fermi 2 plant. CECo would also provide an updated Quad Cities ECCS analysis report to replace Reference 4. Attachment 4 to the December 22, 1987 letter (Ref. 5) provides a summary of the available ECCS subsystems for various break locations and failures, including consideration of the design flaw in the swing bus transfer system. The results for the assumed single failure of the DC battery are as follows:

Break Location	Available ECCS Subsystems
Recirculation Discharge or Suction Line	1 LPCS[b] + HPCI + ADS[c]
Low Pressure Core Spray Line	HPCI + ADS
Feedwater Line[a]	1 LPCS + HPCI + ADS 1 LPCS + ADS

(a) Break assumed to occur in feedwater line where HPCI system injects, available ECCS subsystems dependent upon break location.
(b) LPCS - low pressure core spray
(c) ADS - automatic depressurization system

No LOCA analysis results on maximum PCT were presented for the failure of the DC battery power supply for the limiting break size and location and remaining ECCS subsystems.

In response (Ref. 6) to a staff request for additional information (Ref. 7), CECo provided another piece of correspondence relevant to the DC battery failure issue. CECo provided its response to NRC Question II.B.11 in Amendment 11/12 of the Dresden Units 2 and 3 original FSAR. This question was:

II.B.11 Evaluate the ability of your onsite and offsite electrical power systems to each separately, and independently, supply engineered safety feature loads for one unit and safe shutdown loads for the other unit assuming a single failure in each power system. The analysis should include:

(a) Battery failure (250 or 125V dc).
(b) Faulted DC bus (250 or 125V dc).
(c) Faulted transfer devices (ac and dc systems).
(d) Any ac or dc load fault.

The CECo response to this question erroneously stated (although the response was believed to be correct at the time) that for a 125 volt battery failure, the remaining ECCS subsystems would include one core spray and two LPCI trains. No LOCA analyses were apparently required or performed for the assumed failure scenarios. CECo was not able to verify if the same question was asked on the Quad Cities docket.

In Reference 8 CECo discusses the probability and safety significance of the DC battery failure, the application of the Single Failure Criterion (SFC) to its ECCS licensing basis, the planned modifications to correct the design flaw in the DC battery swing bus arrangement at the Quad Cities and Dresden plants, and the revision to its new ECCS analysis for the Quad Cities plants (Ref. 9). CECo reiterated its contention concerning (1) the unlikely sequence of events which must occur in a narrow time frame for a coincident LOCA, LOOP, and DC battery failure, (2) the high reliability of its DC battery system, and (3) its monitoring and surveillance program to ensure the high reliability of the DC battery system. CECo again stated that the assumption of a passive single electric failure was not part of its licensing basis. The revised ECCS report (Ref. 9) merely deletes references to DC battery failures and single passive failures when compared to the previous version of the report (Ref. 4). No new LOCA analyses considering the design flaw in the swing bus transfer arrangement are presented.

Modifications planned by CECo to correct the design flaw in the DC battery swing bus transfer system will be completed for all of the affected plants (Quad Cities Units 1 and 2 and Dresden Units 2 and 3) by the beginning of 1990. However, this raised the issue of whether or not the affected plants are in compliance with the requirements of 10 CFR 50.46 regarding ECCS during nearly a 2-year period needed to implement the necessary modifications.

2.0 BACKGROUND

2.1 Fermi 2 LER 87-045-00

By letter dated October 8, 1987 (Ref. 2), the Detroit Edison Company, the licensee for the Fermi 2 plant, submitted LER 87-045-00 which describes an event which occurred on September 8, 1987 at the Fermi 2 plant as a result of a procedural error. While Fermi 2 was in a cold shutdown condition, an operator removed a fuse which deenergized the DC control power to Bus 72C. This bus is the normal feed to the LPCI swing bus. The loss of DC control power resulted in the loss of the power supply to the swing bus and thus to the LPCI Loop Selection Valves.

Upon removal of the fuse, DC control power was removed from Bus 72C and its associated breakers. The breakers did not change state. Loss of DC control power to Bus 72C position 3C caused the DC coil magnetic contactor in Bus 72C, which feeds the 480 volt alternating current (AC) Motor Control Center (MCC) 72CF, to drop out. This deenergized MCC 72CF. The MCC 72CF LPCI swing bus provides AC motive power and control to seven LPCI Loop Selection, Injection, and Isolation Valves.

The swing bus is normally energized from electrical Division I. When Division I power is lost, a throwover circuit activates standby feed from electrical Division II from Bus 72F position 5C. The design of the throwover circuit required that Bus 72C position 3C and associated DC coil magnetic contactor open. This would provide a permissive to close for Bus 72F position 5C and its associated DC coil magnetic contactor. However, Bus 72C position 3C did not open on loss of DC control power but the magnetic contactor did open, MCC 72CF deenergized, and the throwover was blocked. The Fermi 2 operations shift on duty recognized that MCC 72CF deenergized from alarms and annunciators in the control room and restored power to the swing bus by replacing the fuse. Detroit Edison states that the swing bus lost power for only 5 minutes.

Detroit Edison subsequently determined that a design error in the DC control circuitry for Bus 72C existed. This led to the identification of an event which placed the plant in an unanalyzed condition and thus an unreviewed safety question existed. The event is a LOCA coincident with a LOOP with the single failure of loss of one division of DC power. This event had not been correctly considered in past analyses because of the previously unidentified design flaw. The loss of control over the LPCI valves due to the deenergization of MCC 72CF had not been recognized. The design flaw would lead, upon MCC 72CF deenergization, to the loss of capability of all 4 LPCI pumps to inject coolant into the reactor vessel.

Since a condition had been identified that could have prevented the fulfillment of the safety function of the LPCI system, Detroit Edison took the following corrective actions. It had the General Electric Company (GE) perform an analysis for the degraded ECCS at the then current power level of 50% of full rated power. The maximum PCT was determined to be below the 2200° F limit. Modifications were proposed to correct the design error so that loss of DC power to the normal feed allows the transfer to the standby feed so that MCC 72CF remains energized. In addition, Detroit Edison instituted for its personnel training on the swing bus features and counseling and discipline, as appropriate.

Some additional details concerning this Fermi 2 event may be found in NRC Event Followup Report 87-162 (Ref. 10) and in LER 87-045-00 for the Fermi 2 plant (Ref. 2).

2.2 Acceptability of Swing Bus Design of BWRs

The NRC released a report (Ref. 11) during November 1976 that discussed a number of technical issues. Issue No. 3 concerned the acceptability of the swing bus design of BWR-4 plants. The issue was defined as follows:

> "The swing bus design proposed in BWR-4 plants does not satisfy the single failure criterion. Additionally it violates the independence requirements set forth in GDC 17 and IEEE Std. 308. A single failure at the bus can cause two diesel generators to be paralleled resulting in the loss of two divisions of emergency power and therefore the loss of functional capability to mitigate the consequences of design basis accidents."

The staff response to this issue stated that, for those plants where the swing bus design is permitted, the consequences of a complete failure of LPCI coincident with a LOCA (and presumably a LOOP) are analyzed to assure that the results are acceptable. The staff response went on to say that, where complete LPCI failure coincident with a LOCA (and presumably a LOOP) have not been analyzed, the licensees have either removed the swing bus design or have committed to do so.

The staff reported that Regulatory Guide 1.6 (Ref. 20), developed some time after the BWR-4 swing bus design was accepted by the staff, describes improved ways to perform the safety function provided by the swing bus. The staff stated, however, that backfitting changes on operating plants or plants at the operating licence (OL) stage of review was not justified, except when it would be required to meet ECCS criteria.

The report notes that the swing bus design was introduced by GE for BWR-4s and earlier designs in an attempt to rectify a single failure problem in the fluid system design. In the BWR-4 design, the LPCI function is accomplished by an injection valve in each of the two recirculation loops. The control logic is such that the injection valve for LPCI to the intact loop opens to allow LPCI to begin, with the pipe break in the remaining recirculation loop. This is the so-called LPCI with the Loop Select Logic design. Since the intact loop is not known prior to the event, both injection valves are powered from one electrical bus which can derive power from either of two independent division of Class 1E power. This swing bus design was adopted by GE as a method of removing power source failures from the envelope of single failures.

The staff discussion of this issue states further that the staff accepted this swing bus design because, even though a single failure of the injection valve could disable the LPCI function, the remaining ECCS could cool the core. The remaining staff issue in the review of the swing bus design was to ensure that failures did not propagate to other systems. Thus the swing bus design was limited to only essential LPCI loads. The transfer circuitry between electrical power divisions was also required to be immune to single failure (see previous discussion of Fermi 2 LER on swing bus design flaw).

As a matter of fact, some licensees elected to modify their LPCI electrical systems in order to take credit for a portion of the LPCI flow in their ECCS analyses. The modifications resulted in the use of a split bus design, in accordance with Regulatory Guide 1.6, rather than the original swing bus design. Some facilities were stated as not requiring the modifications since they could meet the ECCS criteria of 10 CFR 50.46. The swing bus design for these plants was not then re-reviewed.

From the staff discussion of this issue, a number of important points can be made:

(1) Plants with the swing bus design and the Loop Select Logic were known to be vulnerable to a single failure in the intact loop (single failure of an injection valve) such that the LPCI function could be totally disabled. This is especially pertinent in light of the design flaw recently noted at the Fermi 2 plant. The very type of failure that the swing bus design was suppose to overcome occurred.

(2) Plants with the swing bus design and the Loop Select Logic were expected and required to meet the ECCS criteria of 10 CFR 50.46 with the ECCS subsystems remaining after the loss of the entire LPCI function.

(3) Plants with the modification of the LPCI electrical system to a split-bus design could take credit for a portion of the LPCI flow in LOCA analyses.

Regulatory Guide 1.6 (Safety Guide 6) provides additional guidance concerning the independence between redundant standby power sources and their distribution systems (Ref. 20).

2.3 Additional Information on the Effect of a DC Power Supply Failure on ECCS Performance

By letter dated November 1, 1978 (Ref. 12), GE responded to a staff concern on the effect of a DC power source failure on the approved 10 CFR 50.46 conformance calculations for operating BWR-3s and BWR-4s. The GE letter presented the results of a study performed with the 1977 approved model and input changes and used bounding assumptions to provide generic results applicable to all operating BWR-3s and BWR-4s. This study considered as one category those plants which retained the LPCI Loop Select Logic. The conclusions of the study were that (1) for small break LOCAs the maximum PCT was higher than previously calculated for the most limiting single failure, (2) the limiting break was the same as previously analyzed, (3) for large break LOCAs the maximum PCT is not affected by a DC power source failure, and (4) the maximum average planar linear heat generation rate (MAPLHGR) for a plant is not affected by a DC power source failure.

Based on the information presented in this GE response (Ref. 12), the staff requested by letter dated April 25, 1980 (Ref. 13) that CECo confirm the conclusions of the study regarding minimum ECCS equipment availability in the event of a DC power supply failure. CECo responded to this request (Ref. 14) and stated that the equipment listed by GE would be available in the event of a DC power supply failure in conjunction with a recirculation loop discharge or suction pipe break. CECo went on to state that modifications were completed at the Dresden station and were underway at the Quad Cities station to ensure that HPCI is available following a DC power failure. The modification provided for automatic transfer from the primary to the alternate 125 volt DC power source.

The GE analysis did consider a coincident LOCA, LOOP, and loss of DC battery power supply. The results presented in the study are directly applicable to the ECCS compliance issue when the recently identified design flaw in the DC swing bus transfer system is corrected. This exchange of letters and the GE study highlight the staff concerns with the BWR-3 and BWR-4 plants' DC power sources and ECCS compliance issue during this time period.

2.4 Single Failure Criterion and ECCS

The Regulations consider the SFC in a number of places that are pertinent to this discussion. In Appendix A to 10 CFR 50, the SFC is defined in the following manner:

> Single failure. A single failure means an occurrence which results in the loss of capability of a component to perform its intended safety functions. Multiple failures resulting from a single occurrence are considered to be a single failure. Fluid and electric systems are considered to be designed against an assumed single failure if neither (1) a single failure of any active component (assuming passive components function properly) nor (2) a single failure of a passive component (assuming active components function properly), results in a loss of the capability of the system to perform its safety function.*

with an explanatory footnote added:

> * Single failures of passive components in electric systems should be assumed in designing against a single failure. The conditions under which a single failure of a passive component in a fluid system should be considered in designing the system against a single failure are under development.

This definition is relatively straightforward to apply to a simple isolated system. Its application results in a system design with sufficient diversity and redundancy so that a system can perform its intended function in the event of a single random failure.

General Design Criterion (GDC) 35 of Appendix A to 10 CFR 50 addresses ECCS as follows:

> Criterion 35 - Emergency core cooling. A system to provide abundant emergency core cooling shall be provided. The system safety function shall be to transfer heat from the reactor core following any loss of reactor coolant at a rate such that (1) fuel and clad damage that could interfere with continued effective core cooling is prevented and (2) clad metal-water reaction is limited to negligible amounts.
>
> Suitable redundancy in components and features, and suitable interconnections, leak detection, isolation, and containment 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 second part of GDC 35 provides some further amplification of the SFC when applied to the ECCS. It states that the system must have redundancy in components and features, among other things, such that for onsite electric power system operation (assuming offsite power is not available) and for offsite power system operation (assuming onsite power is not available), the ECCS safety function can be accomplished, upon assuming a single failure. Again this version of the SFC is relatively straightforward to apply when only the ECCS is considered in isolation. In particular, no distinction is made in whether the assumed single failure is an active single failure or a passive single failure. There is however an additional feature of importance in GDC 35's rendition of the SFC. This is that suitable interconnections must be provided, presumably between and among interacting fluid and electrical systems when the ECCS function is activated.

The SFC is explicitly treated in Appendix K to 10 CFR 50. In the discussion of post-blowdown phenomena and heat removal by the ECCS, the following is required:

> Single Failure Criterion. An analysis of possible failure modes of ECCS equipment and of their effects on ECCS performance must be made. In carrying out the accident evaluation the combination of ECCS subsystems assumed to be operative shall be those available after the most damaging single failure of ECCS equipment has taken place.

This version of the SFC is very explicit in its requirements regarding the ECCS. It states that an analysis of failure modes must be made and that the accident analysis must consider the most damaging single failure of ECCS equipment. No discussion is provided on whether the single failure needs to include either active or passive single failures. Again the application of this version of the SFC is relatively straightforward when applied only to the ECCS. The application of the SFC to interconnected electrical and other fluid systems is however not treated in this version of the SFC.

Standard Review Plan (SRP) Section 15.6.5 (Ref. 16) addresses the NRC review procedures for the ECCS. SRP Section 15.6.5 Revision 2 was issued in July 1981. It states that the reviewer must assure that an adequate failure modes analysis has been performed to justify the selection of the most limiting single active failure. However, this failure modes analysis appears to be directed to the ECCS and not to system-to-system interactions or to functional dependencies between systems.

A general discussion of the SFC is provided in SECY-77-439 (Ref. 15). This staff information report concludes that the SFC has served the staff well as a tool in the defense-in-depth approach to reactor safety. It also concludes that the results of the Reactor Safety Study (RSS) indicate that application of the SFC has led to an acceptable level of redundancy in most systems important to safety. It notes that problems did exist in specific interpretations and applications of the SFC.

The SECY-77-439 information report makes many observations concerning the SFC. It notes, in particular, that the application of the SFC involves a systematic search for potential failure modes and their effects on the functioning of the system. The objective is to search for design weaknesses which can be overcome by increased redundancy, use of alternate systems, or use of alternate procedures. It considers those systems or components which have a credible chance of failure.

The SECY-77-439 paper notes that the probability of accident sequences resulting in a core meltdown were found by the RSS to be importantly influenced by system-to-system interactions and by functional dependencies between systems. The functional dependencies can be considered as a class of interactions where the functioning of one system depends on the satisfactory functioning of another system. The report concludes that the SFC must be supplemented by additional methods when treating such functional dependencies. The report concludes however that the SFC should continue to be used pending resolution of specific problem areas and the incorporation into the licensing process of reliability and risk assessment methodology.

Regulatory Guide 1.53 (Ref. 18) provides some additional information concerning the SFC. This guide endorses IEEE Std. 379-1972 (Ref. 19) which discusses an industry position on the SFC. The information provided by both RG 1.53 and IEEE Std. 379-1977 (a later version) supplements the information discussed previously. These two documents provide details of the implementation of the SFC to the design of Class 1E systems.

IEEE Std. 379-1977 states that certain conditions are implicit in the application of the SFC to the design of Class 1E systems. One of these conditions is provided in Section 5.1 which states that the principle of independence is basic to the effective utilization of the SFC. In fact Section 5.1 states that a requirement in the design of a Class 1E system is that no single failure of a component will interfere with the proper operation of an independent redundant counterpart system. Section 5.2 of the standard states that the detectability of failures is implicit in the application of the SFC. When nondetectable failures are identified, then the designer can choose either (1) to redesign the system or the test scheme or (2) to assume that nondetectable failure have occurred in the analysis of the system. The first option is the preferred course of action.

3.0 EVALUATION

In the preceding section we have provided background information on (1) the Fermi 2 event (Section 2.1), (2) acceptability of the DC power supply swing bus design (Section 2.2), (3) effect of a DC battery power supply failure on ECCS performance (Section 2.3), and (4) the Single Failure Criterion and ECCS (Section 2.4). The staff's evaluation of these topics form the basis for our conclusions regarding compliance of CECo plants with 10 CFR 50 Appendix A and K. Some of our principal conclusions from the aforementioned sections are as follows:

Section 2.1 Fermi 2 Event

1. A design flaw was identified in the DC battery power supply swing bus transfer system at Fermi 2. This design flaw is a nondetectable failure in IEEE-379-1977 terminology. It compromises a Class 1E system's redundancy features.

2. Modifications have been proposed by Detroit Edison to restore the redundancy features of the DC power Supply swing bus transfer system.

3. Analyses have been performed for Fermi 2, including the effect on available ECCS equipment of a loss of DC power due to a failure of the swing bus transfer system, to establish compliance with the criteria of 10 CFR 50.46 for the current power level limit of 50% of full rated power.

Section 2.2 DC Power Supply Swing Bus Design

1. Plants with the swing bus design and the Loop Select Logic were known to be vulnerable to a single failure in the intact loop (single failure of an injection valve) such that the LPCI function could be

totally disabled. This is especially pertinent in light of the design flaw recently noted at the Fermi 2 plant. The very type of failure that the swing bus design was supposed to overcome occurred.

2. Plants with the swing bus design and the Loop Select Logic were expected and required to meet the ECCS criteria of 10 CFR 50.46 with the ECCS subsystems remaining after the loss of the entire LPCI function.

3. Plants with the modification of the LPCI electrical system to a split-bus design could take credit for a portion of the LPCI flow in LOCA analyses.

Section 2.3 Earlier Analysis of ECCS and DC Power Supply Failure

Earlier GE analyses (References 4 and 12) on the effect of a DC battery power supply failure on ECCS performance is applicable to the present compliance issue concerning CECo's affected plants because the analysis did consider a coincident LOCA, LOOP, and loss of the DC power supply.

Section 2.4 Single Failure Criterion

1. IEEE Std. 379-1977, which is endorsed by Regulatory Guide 1.53 (the 1972 version is endorsed), states that a number of conditions are implicit in the application of the standard. This includes the principle of independence as being basic to the effective utilization of the Single Failure Criterion. Section 5.1 of the standard states, in fact, that no single failure of a component will interfere with the proper operation of an independent redundant counterpart system.

2. Section 5.2 of the standard states that the detectability of failures is implicit in the application of the Single Failure Criterion. When nondetectable failures are identified, then the designer can choose either (1) to redesign the system or the test scheme or (2) to assume that the nondetectable failure has occurred in the analysis of the system. The first option is the preferred course of action.

3. GDC 35 requires an ECCS which is capable of providing abundant emergency core cooling.

4. GDC 35 requires that the ECCS must have suitable redundancy of components and features, among other things, such that for onsite electric power system operation (assuming offsite power is not available) and for offsite power operation (assuming onsite power is not available), the ECCS safety function can be accomplished, upon assuming a single failure.

5. GDC 35 requires that suitable interconnections must be provided. The staff interprets this statement to include interconnections between and among interacting Class 1E fluid and electrical systems.

6. The SECY 77-439 paper notes that the SFC must be supplemented by other methods when system to system interactions and functional dependencies between systems are treated.

The primary conclusion which results from the above conclusions is that a Class 1E system with a nondetectable flaw violates previous staff positions on such systems. The redundancy feature of a flawed Class 1E system is not assured during an accident condition when its operation is required. Therefore, credit may not be taken for a flawed Class 1E system in the analysis of a design basis event. Additional details concerning this staff position follows with respect to the issue of the compliance of affected CECo plants with the ECCS requirements of 10 CFR 50.46.

Licensees evaluate their plants for conditions which include normal plant operations (startup, shutdown, load follow, off-normal conditions, etc.), anticipated operational occurrences (plant transients or disturbances which can occur with a frequency of at least once per forty years), and postulated accidents of low probability (for example, the sudden loss of integrity of a major component). The analyses must include an accident whose consequences are not exceeded by any other accident considered credible so that the site evaluation required by 10 CFR 100 may be performed. Severe accidents of the Class 9 type (successive failures of multiple barriers) are not required to be considered, although the NRC is evaluating and formulating a policy for such accidents. The purposes of this plant evaluation are, among other things, (1) to study the response of the plant under normal, transient, and accident conditions, (2) to define limits on plant process variables (coolant temperature, pressure, flow rate, power distribution including power peaking factors, etc.), (3) to define functional requirements on equipment important to safety, (4) to define functional requirements of monitoring equipment, (5) to aid in the formulation of operating procedures, and (6) to assess the radiological consequences of limiting postulated accidents. The result of such evaluations and examinations of consequences of normal, transient, and accident conditions is to assure the plant's ability to withstand and accommodate these conditions with respect to (1) fuel integrity, (2) reactor coolant pressure boundary integrity, (3) control rod insertability, (4) core coolability, and (5) offsite radiological dose limits. The evaluations that are required for light water reactors (LWRs) are discussed in Chapter 15 of Regulatory Guide 1.70 (Ref. 17) and in Chapter 15 (or equivalent chapter) of a plant's FSAR.

The low probability accident that is postulated to bound the consequences of all other such low probability accidents is LOCA. This event is analyzed over a wide spectrum of small and large pipe breaks at various locations and conditions with models and input assumptions in conformance with the requirements of Appendix K to 10 CFR 50. The analysis is performed so that if offsite power is assumed to be lost then onsite power is considered to be available. Conversely, if onsite power is assumed to be lost then offsite power is considered to be available. A failure modes and effects analysis is made to determine the worst single failure for the pipe break being analyzed so that the remaining available ECCS subsystems can be identified for the LOCA analysis. The worst single failure noted in this analysis is usually an active single failure. The results of these extensive LOCA analyses are used to determine the worst pipe break size and location and the worst single failure. To meet the criteria of 10 CFR 50.46, the results of the analyses are usually expressed as limits on the total power peaking factor or, equivalently, on the linear heat generation rate (LHGR) for PWRs or as a limit on the average planar linear heat generation rate (APLHGR) as a function of exposure for a given fuel bundle type for BWRs.

With regard to the issue of whether or not active or passive failures or both types of single failures need to be treated in a failure modes and effects analysis (FMEA) of the ECCS subsystem, the staff notes that the application of the SFC is difficult and ambiguous with respect to interconnected and interacting systems such as the ECCS. However, it was never intended that interconnected or interacting Class 1E systems should be vulnerable to a single active or passive failure or a nondetectable failure such that the functioning of a particular Class 1E system would be in doubt during a design basis event. The existing LPCI swing bus design flaw, or any other nondetectable failure of the Class 1E DC power supply to the swing bus transfer arrangement, places the DC power supply in this category; that is, its availability will be in doubt during a design basis LOCA.

Since the availability of the Class 1E DC power supply with a non-detectable failure could be in doubt during a critical time period of a design basis LOCA, it is the staff's position that credit for its proper functioning during such an event cannot be assumed in the analysis. Therefore, CECo, when performing LOCA analyses for its Quad Cities and Dresden plants, must assume the coincident failure of the DC power supply in conjunction with a LOCA and LOOP. Thus the additional ECCS equipment not available because of the assumed failure of the DC power supply can not be credited in the LOCA analyses. This additional nonavailable ECCS equipment may result in a design basis LOCA that is more limiting than previous analyses for the Quad Cities and Dresden stations. Consequently, CECo must establish compliance with 10 CFR 50.46 by providing the results of appropriate LOCA analyses which include the loss of ECCS equipment due to failure of any DC power supply.

CECo has also proposed modifications for the Quad Cities and Dresden DC power supply systems to correct design flaws in the swing bus automatic transfer arrangement. The proposed modifications are the subject of a separate staff review contained in Enclosure 1. All four units will be modified over an extended 2-year period with Dresden Unit 3 being the last plant modified during it's December 1989 outage (Ref. 8). However, during the interim time interval required to perform plant modifications, the four CECo units may not be in compliance with 10 CFR 50.46. But, the staff has concluded that CECo need not perform additional LOCA analyses in accordance with 10 CFR 50, Appendix K to account for the existing plant configuration (i.e. with the LPCI swing bus design flaw). Because the probability of a coincident LOCA, LOOP, and unavailability of DC power to the swing bus transfer system is very low during the interim time period necessary to accomplish the planned modifications.

4.0 CONCLUSIONS

The staff has reviewed the DC power supply swing bus transfer arrangement (including the design flaw) with regard to the ECCS performance capability. For reasons discussed in this evaluation, the staff determined that the loss of a DC power supply system must be included as one of the possible single failures in the design basis LOCA analyses. Since CECo has not submitted the results of such analyses to the NRC, we cannot determine that the Quad Cities (1 and 2) and Dresden (2 and 3) stations are in complete compliance with the requirements of 10 CFR 50.46. Consequently, the staff has decided that CECo must establish compliance with 10 CFR 50.46 by conducting appropriate LOCA analyses that encompass single failures in DC power supplies (e.g. loss of a 125 DC Battery, etc.).

Furthermore, regardless of the design modification described in Enclosure 1, the LPCI Swing bus design does not meet the single failure provisions prescribed in 10 CFR 50, Appendix A (i.e. General Design Criteria 35). Consequently, the NRC is currently reviewing the feasibility of issuing an exemption that will address 10 CFR 50, Appendix A compliance.

5.0 REFERENCES

1. Letter from J. A. Silady (CECo) to Thomas E. Murley (NRC), dated December 21, 1987.

2. Letter (NRC-87-0183) from W. S. Orser (Detroit Edison) to NRC, dated October 8, 1987 (this letter transmitted LER 87-045-00, "Low Pressure Coolant Injection Swing Bus Design Flaw Identified by Personnel Error").

3. Letter from J. A. Silady (CECo) to Thomas E. Murley (NRC), dated September 18, 1987 (this letter transmitted a Proposed Amendment for the Quad Cities Unit 1 Cycle 10 Reload).

4. "Quad Cities Nuclear Power Station Units 1 and 2 - SAFER/GESTR-LOCA - Loss of Coolant Accident Analysis," NEDC-31345P, June 1987.

5. Letter from J. A. Silady (CECo) to Thomas E. Murley (NRC), dated December 22, 1987.

6. Letter from J. A. Silady (CECo) to Thomas E. Murley (NRC), dated January 21, 1988.

7. Letter from G. M. Holahan (NRC) to L. D. Butterfield (CECo), dated December 22, 1987.

8. Letter from, J. A. Silady (CECo) to Thomas E. Murley (NRC), dated February 19, 1988.

9. "Quad Cities Nuclear Power Station Units 1 and 2 - SAFER/GESTR-LOCA - Loss of Coolant Accident Analysis," NEDC-31345P Revision 1, January 1988.

10. NRC Memorandum from Wayne D. Lanning to Faust Rosa, dated November 30, 1987 (this memorandum has attached Event Followup Report 87-162).

11. "Staff Discussion of Fifteen Technical Issues Listed In Attachment to November 3, 1976 Memorandum from Director NRR to NRR Staff," NUREG-0138, November 1976.

12. Letter (MFN-410-78) from R. E. Engel (GE) to the USNRC, dated November 1, 1978 (this letter presented information on DC power source failure for BWR-3s and BWR-4s).

13. Letter from Thomas A. Ippolito (NRC) to D. Louis Peoples (CECo), dated April 25, 1980.

14. Letter from Robert L. Janecek (CECo) to T. A. Ippolito (NRC), dated June 12, 1980.

15. "Single Failure Criterion," SECY-77-439, August 17, 1977.

16. "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants - LWR Edition," NUREG-0800, July 1981.

17. "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants - LWR Edition," Regulatory Guide 1.70, Revision 2, September 1975.

18. "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems," Regulatory Guide 1.53, June 1973.

19. "IEEE Standard: Application of the Single Failure Criterion to Nuclear Power Generating Station Class 1E Systems," IEE Std. 379-1977, June 30, 1977.

20. "Independence Between Redundant Standby (Onsite) Power Sources and Between Their Distribution Systems," Regulatory Guide 1.6 (formerly Safety Guide 6), March 10, 1971.

Principal Reviewer: D. Fieno

Dated: October 13, 1988