



UNITED STATES  
NUCLEAR REGULATORY COMMISSION

WASHINGTON, D.C. 20555-0001

April 4, 1995

Mr. Mike Barrett  
Duke Power Company  
P.O. Box 1006  
Mail Code EC08I  
Charlotte, NC 28201-1006

Dear Mike:

We have enclosed our comments and questions on the Draft Keowee PRA. Additional comments and questions may be forthcoming since we are still continuing a fault tree review.

We request your responses to these comments and questions in an informal letter report. If you have any questions, please call me at 301-415-1082.

Sincerely,

A handwritten signature in cursive script that reads "Stacey L. Rosenberg".

Stacey L. Rosenberg,  
Reactor Systems Engineer  
Probabilistic Safety Assessment Branch  
Division of Systems Safety and Analysis

9606240108 960621  
PDR ADOCK 05000269  
P PDR

9606240108

Bayesian updating  
EPRI CRPS  
Smart Lewis-concurring  
O failures; error factors  
don't change

**Preliminary Comments**  
on the  
**Draft Oconee Nuclear Station**  
**Keowee Reliability Analysis, Volume 1**  
**Duke Power Company, December 1994**

**SCIENTECH, Inc.**  
**March 1995**

Cont. call about  
Bayesian updating

Written comments - 2 wks from

The comments presented below are based on an initial review of Volume 1 of the draft Oconee Nuclear Station Keowee Reliability Analysis, Duke Power Company, December 1994. No attempt has been made to prioritize the comments.

Preliminary Comments Draft Oconee Nuclear Station Keowee Reliability Analysis, Volume 1 Duke Power Company, December 1994		
Number	Location Page No.                      Section	Comment
1.	General comment	<p><u>Keowee reliability under different accident conditions.</u> A major objective of the PRA as stated by the authors is to create an integrated reliability model of Keowee to serve as the primary source of emergency ac power for the three-unit Oconee Nuclear Station. <del>The function of Keowee is to provide emergency power to Oconee's main feeder buses when normal and offsite power to the plant is lost.</del> Keowee units provide power to the Duke grid and one of them interfaces with the Oconee main feeder buses through the switchyard. This means the latter unit itself can be affected by the nature of the loss of offsite power that Keowee is supposed to mitigate.</p> <p>For Oconee a failure in the switchyard is a LOSP condition to which Keowee is supposed to respond by providing emergency power. When the switchyard does not fail, Keowee can provide emergency power to Oconee from two redundant pathways, neither of which is needed. When the switchyard does fail, however, Keowee has only one pathway to Oconee using the CT4 transformer.</p> <p>Coding a single reliability estimate for Keowee is misleading. Instead, the reliability of Keowee to power the Oconee main feeder buses should be addressed based on each of the particular accident conditions to which Keowee is called upon to respond. Please specify the reliability of the Keowee under different LOSP conditions. →</p>
2.	General comment  <i>Annual Average Average</i>	<p><u>Keowee reliability under different configurations.</u> The authors built the Keowee PRA model by combining into a single model several configurations (CFGs) of the Keowee including the following:</p> <ul style="list-style-type: none"> <li>• Both Keowee units are in maintenance 0.5% of the time;</li> <li>• Keowee Unit 2 is in maintenance 3.8% of the time and Unit 1 is in standby and aligned to the underground path;</li> <li>• Both Keowee units are available; Unit 1 is always in standby and aligned to the underground path. Unit 2 is either in standby aligned to the overhead path 97.6% of the time or it produces to the grid and is aligned to the overhead path 2.4% of the time.</li> </ul>

*Should be 93.3 says Mike*

*They never used this anywhere*

**Preliminary Comments**  
**Draft Oconee Nuclear Station Keowee Reliability Analysis, Volume 1**  
**Duke Power Company, December 1994**

Number	Location		Comment
	Page No.	Section	
2. (cont'd.)	General comment		<p>We believe the model has several shortcomings:</p> <ul style="list-style-type: none"> <li>• The reliability estimates obtained are driven by the probabilities assigned to the above configurations. These probabilities are based on past operating practices that may change in the future. Operating patterns are not part of the Tech Specs and therefore are not required by license;</li> <li>• The sum of the probabilities of all of the configurations exceeds unity;</li> <li>• Not all of the configurations of the Keowee units are accounted for in the model;</li> <li>• Potential conflicts exist in the assumptions governing each configuration, e.g., the position of ACB2 depends on whether Unit 2 is in standby or is producing to the grid; and</li> <li>• Failure modes associated with <del>low-probability</del> <sup>re state</sup> configurations will result in artificially low occurrence probabilities. A failure resulting from low-probability configurations will be subsumed as a small contributor to the overall failure probability. The cutsets associated with the configurations in which one or both Keowee units are producing to the grid are reduced by almost two orders of magnitude. This is because the PRA assumes these configurations are infrequent.</li> </ul> <p>The more rigorous approach that we recommend is to develop a framework to evaluate the reliability of the Keowee units in all of their possible configurations as sources of emergency ac power for Oconee and to obtain the conditional reliability along with the dominant failure modes associated with each configuration. The reliability model for a particular configuration could then be used to perform comparative studies, e.g., of the reliability of the overhead path as compared with the underground path. Such comparative studies are more realistic when they are based on a model governed by common assumptions.</p>
3.	p. ES-3 Paragraph 3	Executive Summary	<p>The authors provide reliability estimates for both the Keowee underground and overhead paths without addressing the alignments of the generators from which the estimates derived.</p> <p style="text-align: center;">N/A</p>

*check on conf. call*

**Preliminary Comments**  
**Draft Oconee Nuclear Station Keowee Reliability Analysis, Volume 1**  
**Duke Power Company, December 1994**

Number	Location		Comment
	Page No.	Section	
4.	Table ES.4-1		The text of "Note 1" should clarify the boundary of the Keowee emergency power with respect to the Oconee MFBs.
5.	p. 2-4 Paragraph 2		Is it necessary to trip the 6.9 kv reactor coolant pump motor buses from the startup transformer to ensure the success of the overhead path? If so, does the PRA model this?
6.	p. 3-4		Spurious actuation of the CO <sub>2</sub> fire protection system can cause generator lockout. Is such actuation modeled?
7.	p. 3-7		Please specify the positions of ACBs 5, 6, 7, and 8 under the following conditions: Units 1 and 2 are in standby with no LO SP; Units 1 and 2 are in standby when LO SP occurs; Unit 1 is in standby and Unit 2 is generating to the grid with no LO SP ; Unit 1 is in standby and Unit 2 is generating to the grid when LO SP occurs; and Units 1 and 2 are generating to the grid when LO SP occurs. When Unit 2 is generating to the grid, how is the 600 V switchgear 2x energized? Please specify the positions of ACBs.
8.	p.4-2 Paragraph 4		Why is the failure of Generator ACB Air system treated as a basic event? What failure probability was assigned to this basic event and what was the basis for this value?
9.	p. 4-6		Please justify Assumption 5.
10.	p.4-7	Section 4.5 Bullet 3	The model is developed based on the configuration as stated in Assumption 1 in Section 4.4.3. How can various Keowee operating modes be incorporated using a model that is predicated on a fixed configuration?
11.	p. 4-8 Paragraph 2	Section 4.6.1	The PRA does not cite the dependency of the CX transformer on the Oconee 1 main feeder buses nor the dependency of Oconee 1 on Keowee as the important circular logic. Please describe the modeling approach employed in the PRA.

*Mention  
TEK*

*ASK about  
at Conf.  
call*

*O.K.*

*O.K.*

*O.K.*

*w/# 2*

*in Conf.  
call - ask  
them to  
state this*

*as an  
example*

*this sentence is still too vague*  
 March 31, 1995

*They think they missed this - they are investigating this.*

**Preliminary Comments**  
**Draft Oconee Nuclear Station Keowee Reliability Analysis, Volume 1**  
**Duke Power Company, December 1994**

Number	Location		Comment
	Page No.	Section	
12.	p. 4-10 Paragraph 3	Section 4.6.4 <i>in conf-call ask them to discuss this</i>	The PRA refers to the use of a rule file to automatically process the cutsets with recoverable basic events. The PRA should discuss the rules used for recoveries.
13.	p.4-12	Section 4.8.4.2 <i>OK</i>	The PRA refers to the 10/92 incident without providing any background information. Many readers may not be familiar with the incident. Please provide references for the reader.
14.	p. 4-14	Section 4.8.8 <i>OK</i>	In the base case, the estimate of time-averaged unavailability of the components of the standby unit is based on 360 hours of exposure time. For a grid-cycled unit the exposure time is assumed to be 12 hours. As part of a sensitivity case, when both units can generate to the grid, the PRA assumes an exposure time of 12 hours. This implies that on average many components of each unit are challenged every 24 hours. Considering that both units can generate to the grid about 3% of the time, how is it possible to challenge each unit every 24 hours?
15.	p. 5-3	<i>OK</i>	It is not clear how the PRA study benefited from the operational data at the Jocassee hydroelectric station.
16.		Table 5.2.1 <i>OK</i>	When did Duke stop using both generators for peaking power?
17.	p. 5-4	Section 5.2.3	The PRA claims that the probability of an emergency start (ES) failure is 4.5E-3. This value was obtained by dividing the number of grid generation start failures reported between 1984 and 1993 by the number of grid generation start demands in the same period.  We believe this value is misleading because it does not take into account the emergency nature of the demand exclusively. This value serves more appropriately as the Keowee start reliability for grid production. Realistically, the start failure probability of Keowee as Oconee's emergency ac power source should be based solely on the number of ES failures experienced and the number of ES demands (actual or test). These values can be obtained from Tables 5.2.1 and 5.2.2 of the PRA report. The number of ES demands is 113 (hot and cold starts). The number of ES failures appears to be 2. These numbers yield an ES failure probability of 1.8E-2.
18.		Table 5.2.2 <i>OK</i>	How did the team apply the number of (hot and cold) ES demands?

*Talk to Virgil  
about this  
Controversial  
Issue*

**Preliminary Comments**  
**Draft Oconee Nuclear Station Keowee Reliability Analysis, Volume 1**  
**Duke Power Company, December 1994**

Number	Location		Comment
	Page No.	Section	
19.		Table 5.2.2 <i>O.K.</i>	Our review shows that the Keowee units actually generated power 386 times in 1989. There also were 155 starts with no power generation. Why does the PRA code 658 demands? Please reconcile the difference between these two startup numbers. <i>Some were maint. &amp; surveillance (work) in one # &amp; not the other - they will look into it.</i>
20.	p. 5-7	<i>O.K.</i>	<u>Plant-Specific Failure Rates</u> . If Bayesian updating is used, what is the purpose of assuming 1 in 2x demands in cases where no failures are reported? What is the utility of plant-specific component failure rates in the PRA?
21.	p. 5-7	<i>O.K.</i>	<u>Results of the component data analysis</u> . The authors state that the <u>plant-specific failure rates are substantially lower than the generic failure rates</u> . They also state "when viewed as an aggregate the Keowee component data is consistent with the generic data." What do they mean by this statement?
22.	p. 5-7	Table 5.3-1 <i>O.K.</i>	Why are the plant-specific failure rates and the updated failure rates labeled as failure probabilities?
23.	p. 5-7	Table 5.3-1 <i>O.K.</i>	In many cases the error factor obtained after the updating process is the same as the generic failure rate "EF." For example, the following values are presented for the failure of a pressure switch to close on demand:  Generic Value : 2.6E-4 EF: 8.1 Updated Probability: 2.9E-6 EF: 8.1  Please explain why the values for the EFs are the same. (See also Comment 50.)
24.	General comment	<i>Check w/ Mike on comp. call</i>	The PRA does not justify the values used for the total number of demands or total number of hours. These values are referred to in the PRA as "denominator values." Does the PRA assume that all similar components (modeled as type codes) have been subjected to the same number of challenges in the last 10 years? Yet <u>Stepup Transformers and Transformer CT4s</u> , for example, are not subject to the same number of demands.

*check send report*  
*Ob they really use this word*

*we knew the answer to this*

**Preliminary Comments**  
**Draft Oconee Nuclear Station Keowee Reliability Analysis, Volume 1**  
**Duke Power Company, December 1994**

Number	Location		Comment
	Page No.	Section	
25.		Table 5.3-1	The number of demands for circuit breakers (PCBs) for type codes "CHC" and "CHO" differ by a factor of 5. Please explain this difference in demand.
26.		Table 5.3-1 <i>O.k.</i>	We assume that failure rates for individual events were calculated using type-code updated failure rates. According to Table 5.3-1, the updated failure rate for the "RYD" code is 3.5E-5 per demand. In Table A.2-5 the value of 2.8E-5 is used to quantify the "S27XTD2RYD" event. How does the PRA team explain this discrepancy?
27.	p. 5-9 Paragraph 4		What is the meaning of the last sentence in this paragraph: "The random failure probability is generally taken as the gate solution."?
28.	p. 5-9 Final paragraph	<i>O.k.</i>	How does daily operation of one generator reduce the common cause failures of two generators? Is the sensitivity study based on generic data using generic MGL parameters?
29.	p. 5-10		For so-called "strongly defended" components the PRA reduces the generic beta factors by a factor of 2. What is the rationale for this reduction in value? Considering the fact that the results are dominated by common cause failures, the effect of the reduction should be assessed.
30.	p. 5-10	Section 5.4.3 <i>O.k.</i>	It is not clear how the system-level common cause analysis was performed. If actual operating data were used as is suggested in Figure 5.4-1, what roles do the generic and Keowee beta factors play in the analysis?
31.	<i>Review this in final report</i>	Table 5.3-1 p. 3 of 4	The PRA reports the total number of failures reported for relays as eight, i.e., five demand failures and three run time failures. Figure 5.2-2 reports 28 failures related only to X Relay failures. How does Duke explain this apparent discrepancy? Does the PRA discount certain failures because relays have been replaced with new devices? If, so, what is the basis for the discount? Did Duke adjust the number of demands or run times to reflect limited experience with the new devices? If not, this practice is not conservative and should be reassessed.
32.	p. 5-14	<i>O.k.</i>	Please provide an example of a post-maintenance error involving a component that is not tested functionally, but is checked daily. What procedures take place during the check?

*They think they must have done this they are going to fix this*

**Preliminary Comments**  
**Draft Oconee Nuclear Station Keowee Reliability Analysis, Volume 1**  
**Duke Power Company, December 1994**

Number	Location		Comment
	Page No.	Section	
33.	General comment	Section 6 <i>O.K.</i>	The PRA classified three classes of LOOP events according to the different impacts they have on the reliability of Oconee emergency ac power. At a minimum, the authors should have provided the failure probability of emergency ac power for each class of LOOP event. Instead, they provided only a single failure probability value for the loss of emergency ac power to Oconee buses.
34.	p. 6-4	Section 6.3 Figures 6.3-6.13	To what extent are the dependencies of the modules "NSFSSF0(6)REC" on support systems modeled? Are the fault trees included in the draft PRA?
35.	p. 7-2 Paragraph 3	<i>N/A</i>	<p>The PRA states that "when both Keowee units are taken out of service, the standby buses are energized by CT5 and [the] 100 kv line [is] energized by starting a Lee combustion turbine unit, thus improving the reliability of the backup emergency power source."</p> <p>This implies that when both Keowee units are undergoing maintenance other sources of emergency power are available in addition to Lee Station, although this is not so. The reliability of emergency power depends entirely on the reliability of Lee Station.</p>
36.	p. 7-2 Paragraph 4		<p>The PRA suggests that the underground path is more reliable than the overhead path. The failure probability of the underground path is estimated to be 0.036. The failure probability of the overhead path is estimated to be 0.074. (The value does not take into account the LOOP conditions that disable the overhead path.) All single unit unavailability is attributed to the overhead unit. The value for maintenance unavailability is 0.038, which is the difference between the failure probability of the overhead and the underground paths.</p> <p>The PRA results imply that when both Keowee units are available the reliability of the overhead power path is the same as the reliability of the underground power path. The modeling differences between the two paths are as follows:</p> <ol style="list-style-type: none"> <li>1. The unit dedicated to the underground path is assumed to be in standby mode all of the time; the unit dedicated to the overhead path is assumed to be in standby 97.6% of the time and generating to the grid 2.4% of the time. Thus the PRA results are driven by a configuration in which both units are in standby.</li> </ol>

*need to check to see if they included NSP → unavailability of SSF A*

**Preliminary Comments**  
**Draft Oconee Nuclear Station Keowee Reliability Analysis, Volume 1**  
**Duke Power Company, December 1994**

Number	Location		Comment
	Page No.	Section	
36. (cont'd.)	p. 7-2 Paragraph 4		<p>2. The exposure time of the unit dedicated to the underground path is assumed to be 1 month; it is assumed to be 1 day for the unit dedicated to the overhead path. For certain run time types of components of the overhead path, this translates into higher reliability than for components of the underground path. The <math>\delta</math> increase needs to be evaluated.</p> <p>3. Excluding auxiliary power, the underground power path requires ACB 3(4) (no change of state) and Transformer CT4; the overhead path requires the Stepup Transformer and the operation of more than 10 circuit breakers and associated relays (that are configuration-dependent). This results in a lower reliability of the overhead power path than the underground power path. This is because the lockout components of the overhead path are of the demand type.</p> <p>Are the <math>\delta</math> increase (described in 36 (2) above) and the <math>\delta</math> decrease (described in 36 (3) above) in the reliability of the overhead path comparable? The demand-type of components specific to the overhead power path appear to be modeled as very reliable compared with generic values. The sensitivity of the PRA results to the reliability of circuit breakers and associated relays needs to be studied.</p>
37.	<i>Have you Mention to Mike</i>	Table 7.5-1 <i>[Signature]</i>	<p>Based on generic data, failure probabilities associated with the "OVERO" and "UNDERO" gates are <math>9.4E-2</math> and <math>5.9E-2</math>, respectively. Ignoring maintenance unavailability which is 0.036, the failure probability of the OVERO gate is 0.058. This implies that the overhead power path is more reliable than the underground power path. Please explain.</p>
38.	p. 7-2	ref. Figures 7.2-3-7.2-4 <i>O.K.</i>	<p>To what configuration of Unit 2 does the ranking apply (i.e., grid generation or standby)? Was a similar importance ranking performed for the unit dedicated to the underground path? If so, are there any differences in the rankings?</p>
39.	p. 7-2	<i>O.K.</i>	<p>Was an importance ranking performed for the top node of the Keowee model? If so, where is the list?</p>
40.	p. 7-3 <i>Disagree</i>	Section 7.3	<p>The PRA calculates the probability of all ac power failing at an Oconee unit to be <math>5.8E-5</math>. The PRA should state explicitly the failure probability of 0.01 that is assumed for Lee Station. The reliability of Keowee is estimated to be 0.01 (before recovery) as well. Can the PRA justify the same reliability for Lee Station?</p>

**Preliminary Comments**  
**Draft Oconee Nuclear Station Keowee Reliability Analysis, Volume 1**  
**Duke Power Company, December 1994**

Number	Location		Comment
	Page No.	Section	
41.		<p><i>Need this to mention in final report.</i></p> <p>Table 7.3-2</p> <p><i>OK</i></p>	<p>We believe a conservative screening value is more appropriate in the absence of a rigorous reliability analysis of the Lee Station <i>★</i></p> <p>The PRA should describe the top ranked events more quantitatively than it does and draw conclusions with respect to different ranking schemes. Based on the FV ranking, the probability of loss of emergency power is almost the same whether one or both Keowee units are undergoing maintenance. What is the explanation for this?</p>
42.		<p>Table 7.2-3</p> <p><i>OK</i></p>	<p>The PRA should define Oconee's power source and Keowee's power path. What are the components of each?</p>
43.	p. 7-4	<p>Section 7.5-1</p> <p><i>OK</i></p>	<p>The PRA states that the more a particular gate value is dominated by specific data the smaller the change in value when generic data are used. The PRA also states that large increases in value are observed in most of the gates when generic data are used. These two statements appear to contradict each other.</p>
44.	p. 7-4	<p>Section 7.5.2</p> <p>Table 7.2.5</p>	<p>When Unit 2 is aligned with the overhead path and is generating to the grid, ACB 2 is closed. If an emergency start is demanded, it is our understanding that ACB 2 needs to open as part of yellow bus isolation and to reclose. Therefore failure to open ACB 2 should be a single cutset in the overhead path. This cutset does not appear in the table. Please explain why not.</p> <p><i>to be case of w/comm #2</i></p>
45.		<p>Section 7.5.2</p> <p><i>resolve w/ m.ke @ conf call</i></p>	<p>Throughout the report and in this section in particular the PRA report states that the grid-cycled unit is more reliable than the standby unit. The authors' narrative explanation as to why this is believed to be the case is informative. Do they have any statistical data to support this finding? When an emergency start demand occurs is the grid-cycled unit equally reliable whether it is in grid-generation or in standby mode?</p> <p>The authors should also discuss the reliability models they used. At a minimum they should pick several representative components from the standby unit and their counterparts in the grid-cycle unit and explain how the PRA quantified the failure probabilities of each. The unavailability expressions that were used and their associated parameters (e.g., exposure time, repair time) also need to be discussed.</p>

**Preliminary Comments**  
**Draft Oconee Nuclear Station Keowee Reliability Analysis, Volume 1**  
**Duke Power Company, December 1994**

Number	Page No.	Location Section	Comment
46.		Section 4.1.1	In conclusion 3, the excitation system is cited as the main source of unit failure. While it is a main source, the circuit breakers can also be a critical source of failure because they allow the cold and hot starts for each unit. The reliability of each unit's start sequence is very sensitive to the reliability values attributed to each ACB and PCB. See Appendix A for more on this point.
47.		Section 4.1.2	<p><u>Use of Keowee for Grid Generation.</u> According to conclusion 1 in this section the Grid-Cycling unit is more reliable than the Standby unit. The results of SCIENTECH's own sensitivity studies cause us to question this conclusion. (See Appendix A.)</p> <p>In Conclusion 2 it is stated that Keowee Unit 2 "may be started almost daily." What do the qualifiers "may" and "almost" mean precisely? KU2 is taking credit for daily generation.</p>
48.	General comment	<p><i>We think as a concern of final report</i></p>	<p><i>Consideration of the potential for electrical systems interactions between the various Oconee Units and Keowee is not considered.</i> The Oconee Nuclear Station is unique among U.S. nuclear power plants in the use of a hydroelectric dam to supply emergency power to three separate nuclear power plants via a pair of common emergency buses. The obvious safety question in such a configuration is: Given a loss of normal power supplies or loss of offsite power, can a malfunction originating in one nuclear unit cause a problem in an adjacent nuclear unit via the common emergency bus? This critical question is directly avoided in the scope of the analysis. (See Appendix B.)</p>
49.	General comment	<p><i>O.K.</i></p>	<p><i>The scope of functional testing of the undervoltage/underfrequency protection logic is unclear.</i> The fault summary information indicates that various types of logic tests are performed at various intervals. It is unclear whether the tests confirm the operability of individual redundant portions of the logic or if they confirm simply that at least one portion of the logic is operable (See Appendix B.)</p>
50.	General comment	<p><i>O.K.</i></p>	<p><i>The component reliability data used in the Keowee PRA reflect a reduction in generic failure rates that is not possible using Bayesian updating and given the small additional experience observed at Oconee/Keowee.</i> Two examples from Table 5.3-1 make this clear:</p>

**Preliminary Comments**  
**Draft Oconee Nuclear Station Keowee Reliability Analysis, Volume 1**  
**Duke Power Company, December 1994**

Number	Location		Comment
	Page No.	Section	
		→	<p>Example one: The rate of the circuit breaker failing to close is lowered from 1.2E-03 (EF=4) to 9.4E-04 (EF=4) based on no observed failures in 222 demands.</p> <p>It is not possible to lower a failure rate on the order of 1/1000 using on the order of 200 events.</p>
51.	General and specific comments	Human reliability	See Appendix C.
52.	General comment	Data	See Appendix D.

## **APPENDIX A**

### **Independent Reliability Assessment of Keowee Supplying Emergency AC to Oconee (Draft)**

**SCIENTECH, Inc.**  
March 1995

APPENDIX A

A-1. CONSTRUCTION OF KEOWEE MODEL IN REVEAL\_W™

A-1.1 Purpose and Scope of Model

The Keowee Hydroelectric Station was modeled in REVEAL\_W™ to provide an independent assessment of its reliability as a source of emergency power for the Oconee nuclear plants. [1] As discussed in the draft report, a Duke Power Company Fault Tree model already calculated this reliability. [2] The REVEAL\_W™ model duplicated the Duke model and was enlarged to permit analysis of configurations and scenarios that the Duke model did not address.

Because an analyst must be able to focus on individual plant configurations in order to address the failure modes specific to each, the REVEAL-W™ model permits the analysis of the Keowee units in all 13 of their possible configurations. By contrast, the Duke model could analyze only seven configurations and had to process them collectively. Many important failure modes were therefore masked because certain configurations occur with relatively low frequency based on historical data.

Analyzing the 13 configurations proved useful when revisiting the results of the draft report. Before the results are discussed, the differences between the two models are described in more detail.

A.1.2 Problems in Fault Tree Model

A.1.2.1 Failure to Address All Configurations

The Keowee Hydroelectric Station consists of two 87.5 MWe hydroturbine-generators. Each of these generators can operate in five different states, combining to form 13 configurations, as displayed in the following table:

**Keowee Unit 1 Operating Mode**

		M	SU	SO	GU	GO
Keowee Unit 2 Operating Mode	M	☐	☐	☐	☐	☐
	SU	☐	☐	☐	☐	☐
	SO	☐	☐	☐	☐	☐
	GU	☐	☐	☐	☐	☐
	GO	☐	☐	☐	☐	☐

SO: In standby-aligned overhead      GO: Generating to grid-aligned overhead  
 SU: In standby-aligned underground      GU: Generating to grid-aligned underground  
 M: In maintenance

Error

Figure A-1. Possible Configurations of Keowee

The configurations that are grayed out in the table were not addressed by the Duke Fault Tree model, for they were considered to be parallel to the configurations where the units were reversed. Each remaining configuration received an occurrence probability, and these seven configurations were combined into a single fault tree model. Because any grid generation occurs only a small fraction of the time (the units are used for peaking power), any failure mode that results from grid generation will disappear from the cutsets in the final result.

The REVEAL\_W™ model includes several switches, which allow analysis of one configuration at a time. Once analyses are completed, their results can be combined with the conditional probabilities to yield the same final result as the Duke Fault Tree model yields. In the process, however, many insights into the dynamics and sensitivities of the Keowee Station are made available that would otherwise be ignored.

#### **A.1.2.2 Failure to Address Limited Configurations Accurately**

The seven configurations in the Duke model were used to form conclusions in the draft report. Keowee Unit 2 became synonymous with the "Grid-Cycling" unit and Keowee Unit 1 became synonymous with the "Standby" unit, when, in fact, either unit can take on either role. These roles differ depending on the pathway to which the unit is assigned: Hot Starts and Cold Starts are more distinguishable on the overhead pathway, for instance. The simplification of the model used to produce the results in the Duke Power draft report clouds many of the real issues involved in deciding whether an additional unit should generate to the grid. This is addressed later in in this appendix.

#### **A.1.2.3 Failure to Isolate Cutsets of Individual Configurations**

The draft report contains many lists of cutsets that the Fault Tree model produced; the key events associated with grid-cycling are missing. This is because generation to the grid only occurs about 3% of the time that a unit is assigned to the grid. In terms of overall system reliability, the added risk of generating to the grid cannot be detected. In terms of understanding system dynamics, however, the change in risk when a unit generates to the grid must be recognized. For that reason the cutsets associated with each applicable configuration were generated using the REVEAL\_W™ model.

#### **A.1.3 Structure of REVEAL\_W™ Model**

##### **A.1.3.1 Configurations: High Level**

Because the model developed in REVEAL\_W™ is able to quantify all 13 possible configurations of the system, the high-level logic tree looks very different than it does in the Fault Tree model. Expanding to 13 configurations is important because two configurations that are considered symmetrical in the Duke model may respond differently to the same emergency start demand.

The new high-level tree is successful when either Keowee 1 or Keowee 2 supplies power to Oconee and the configuration used to supply the power is allowed. Each generator (Keowee 1 and 2) has the logic shown in Figure A-2.

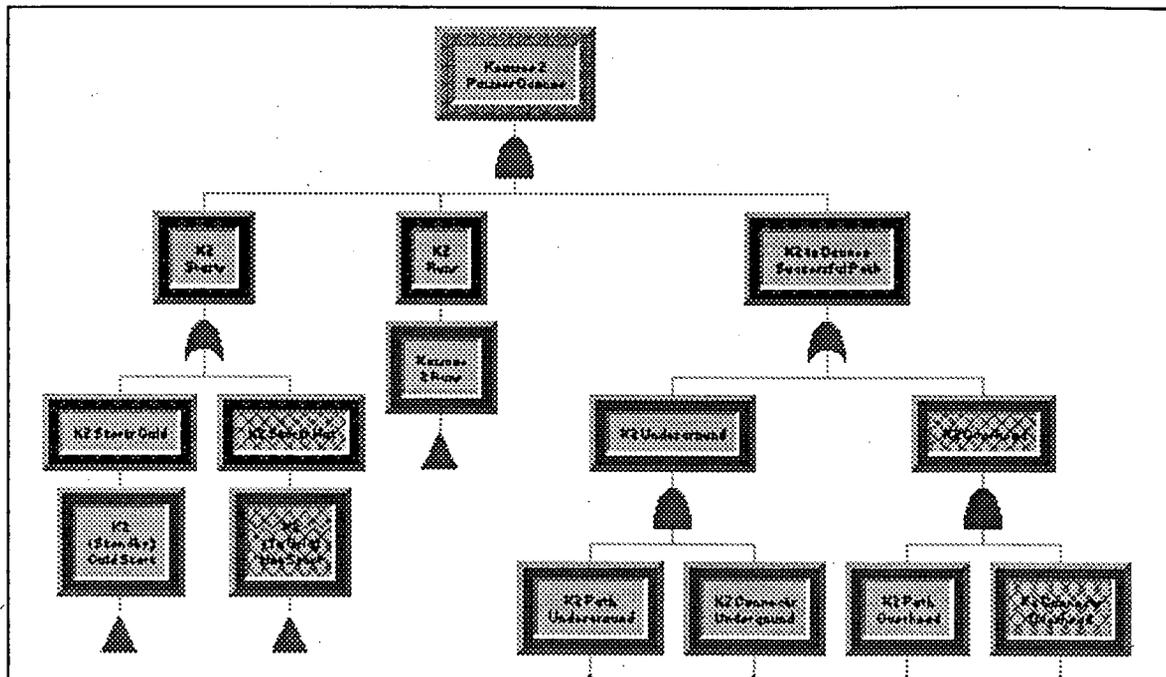


Figure A-2. Logic tree (in success space) for Keowee Unit 2 success

Each unit has three required success branches: successful start, successful run, and successful path to Oconee. If a unit was generating to the grid, it must complete a hot start. Otherwise, it must complete a cold start. The branch that is irrelevant is failed, i.e., the model will not give credit to it. Once a unit has started, it must run. The power path must be completed successfully either underground or overhead. The pathway not under consideration is failed. Figure A-2 illustrates that KU2 is currently in standby and aligned to the underground pathway.

#### A.1.3.2 Configuring the System

Each Keowee unit has three "condition" block (event): The first block indicates whether the unit is aligned to the overhead or underground path. The second block indicates whether it is producing to the grid, and the third indicates whether it is in maintenance. The "state" trees indicate the state of each generating unit. Five states are possible for each generating unit and these are the roots of the trees. For each generating unit, all but one tree will have a root node that is in a "false" state. The tree that is not false indicates the current state of the generating unit.

Of the 25 unit state combinations possible, only 13 configurations are allowed. Whether the particular configuration chosen is allowed is displayed in the tree family called

"Allowed Configurations." The root of this tree is in a false state whenever a disallowed configuration has been selected.

Four main ACBs surround the two generator units (ACB 1,2,3 and 4). The state (open or closed) of these ACBs is a function of the generator configurations. The tree family "Results of Configurations" contains logic that determines the state of these four ACBs.

### **A.1.3.3 Running an Analysis**

To run an analysis, the first step is to choose one of the 13 possible configurations. This involves selecting the "States 1" or the "States 2" tree family in the "Configurations" group. According to the state of the three condition blocks in each tree family, each Keowee Unit can (1) align to the underground or overhead path, (2) generate to the grid or remain in standby mode, and (3) be placed in maintenance. The tree group "Allowed Configurations" will indicate whether the configuration chosen is permissible.

Once an analysis is run, the goal "Keowee Powers Oconee" will show the failure probability of the configuration chosen.

### **A.1.4 Deviations of Logic in REVEAL\_W™ Model**

#### **A.1.4.1 The ACB Trees: Why Additional Logic Was Created**

Additional ACB trees were created to expand the potential configurations from the 7 previously modeled to all 13 possibilities. Once this was done, each of the four generator ACBs (1-4) had three trees: (1) "Ability of ACB(x) to Open," (2) "Ability of ACB(x) to Close," and (3) "ACB(x) Does Not Transfer Open". The tree groups of each ACB were intended to be structurally similar.

The actuations necessary to close ACB 3 and 4, however, are rather different when using the Duke Fault Tree as opposed to the REVEAL\_W™ model. The solution was to provide *both* actuation trees for *each* ACB. The appropriate logical structure was then applied, depending on the chosen configuration. The result is depicted in Figure A-3.

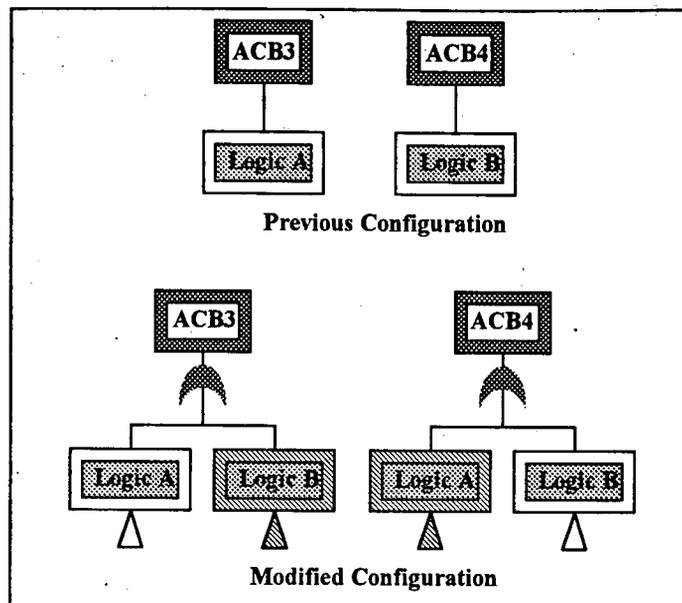


Figure A-3. Modified ACB actuation trees

When a configuration is chosen from the Configuration Group, the dependencies toggle, and the correct branch is relied on. This produces the same probability of failure that the Duke Fault Tree model logic does, but allows for all plant alignments.

#### A.1.4.2 Simplifications

In several areas of the Duke Fault Tree model components are included that do not have a bearing on the final result. For instance, among the "External Grid Protection System Group" fault trees, several trees depict the potential failure of undervoltage or underfrequency signals located on pages 5, 6, 12, and 13 of the report. Each page is composed of 15 basic events, and each one has a duplicate, so that the logic tree on each page has 30 basic blocks. These blocks are used *nowhere else in the model*. Each block has a failure probability of E-5, but when the whole tree is evaluated, it is shown to have a failure probability of 5.9E-8. In other words, the whole tree is insignificant from a risk assessment perspective.

In applying the REVEAL\_W™ model, such a tree was replaced with a single composite block whenever it was encountered. In this case, 120 blocks were replaced by four. They could have been left out altogether without changing the model results.

## A.2. REPRODUCING THE RESULTS OF THE FAULT TREE MODEL

A model of Keowee was constructed in REVEAL\_W™ to (1) reproduce the top 20 cutsets from the Duke Fault Tree model, and (2) to provide an independent estimate of the Keowee failure probability. Both of these activities were carried out without employing failure recoveries.

### A.2.1 Reproducing Top 20 Cut Sets from Fault Tree Model

As stated in Section 4.6.2 of the PRA draft report, "the initial cut set solution is scrutinized carefully to identify inappropriate cut sets, missing cut sets, or cut sets suitable for recovery treatment. This effort occasionally leads to refinement of the model either at the system level or in the high level logic. Following adjustment of the model and application of recoveries, the final model and model solution are produced."

When the REVEAL\_W™ Keowee model is configured for the base case, the cutsets listed in Table 7.2-2 of the draft Report should be reproduced. If the cutsets match, then the REVEAL\_W™ model is validated, subject to the validity of the Fault Tree model.

Recovery treatment is absent from the REVEAL\_W™ model. Because of this, the probability estimates of individual cutsets differ between the models (i.e., although the contents of the cutsets are the same, the sets themselves may be in slightly different order). In the following table, the top 20 cutsets of the Fault Tree model are compared with the corresponding cutsets in the REVEAL\_W™ model: For this run we treated the maintenance unavailability of Unit 2 as a random event and used the same probability value as in the draft PRA.

Fault Tree Model Top 20 Cutsets				REVEAL_W™ Model Similar Cutsets			
#	Type	Description	p(#)	#	Type	Description	p(#)
2	CC	• Both units' WL filters clogged and failure to recover	1.55E-4 <sup>1</sup>	2	CC	• Both units' WL filters clogged	2.6E-3
3	CC	• Failure of the excitation breakers	1.54E-4	3	CC	• K1Y CRB 1/FIELD K2Y CRB 2/FIELD	1.64E-4
4	CC	• All Keowee aux power breakers	1.09E-4			<i>See Comment</i>	
5	Ind Ind	• One unit in maintenance • KHU-1 voltage adjust failure	9.39E-5	6	Ind Ind	• KU2 in maintenance • K1Y CND VOLTADJ	9.39E-5
6	Ind Ind	• One unit in maintenance • KU1 generator fault on run	8.63E-5	7	Ind Ind	• KU2 in maintenance • GEN EGN 1/R	8.72E-5

<sup>1</sup> This value is different from that obtained using REVEAL\_W™ because it includes "failure to recover" as an event.

7	Ind Ind	• One unit in maintenance • ACB7 fails to close-mechanical	6.62E-5	8	Ind Ind	• KU2 in maintenance • ACB ACB 7/C	6.56E-5
8	CC	• Keowee governors fail to run	6.47E-5	10	CC	• HGT TUR 1,2/R	6.00E-5
9	CC	• Unit voltage regulators fail to start	5.79E-5	9	CC	• K1Y,K2Y CND BSADJVOL	6.20E-5
10	Ind Ind	• One unit in maintenance • KHU-1 base adjust maintains	4.71E-5	11	Ind Ind	• KU2 In Maintenance • K1Y CND BASEADJ	4.69E-5
11	Ind Ind	• One Unit In Maintenance • KU1 Gov Fails to Position Wicket Gates - Run	4.56E-5	12	Ind Ind	• KU2 In Maintenance • HGT GOV 1/WG/R	4.56E-5
12	Ind Ind	• One Unit In Maintenance • KU1 Turbine Fails - Run	4.56E-5	13	Ind Ind	• KU2 In Maintenance • HGT: TUR 1/R	4.33E-5
13	Ind Ind	• One Unit In Maintenance • Keowee Battery Number 1	3.51E-5	15	Ind Ind	• KU2 In Maintenance • DCA BAT 1	3.43E-5
14	CC	• Keowee I&C Power Batteries	2.60E-5	16	CC	• DCA BAT 1,2	2.70E-5
15	CC	• Cooling Water Control Valves	2.37E-5	17	CC	• CWS VLV 1WL,2WL-11	2.46E-5
16	Ind Ind	• One Unit In Maintenance • KU1 Base Adjust Failure	2.34E-5	20	Ind Ind	• KU2 In Maintenance • K1Y CND BSASJVOL	2.12E-5
17	CC	• Keowee Battery Chargers	1.85E-5	21	CC	• Batt Chargers KC1, KC2, 1SBC, 2SBC	1.90E-5
18	Ind Ind	• One Unit In Maintenance • KU1 Supply Breaker - Mech	1.76E-5	22	Ind Ind	• KU2 In Maintenance • K1Y CRB 1/SUP	1.76E-5
19	CC	• Keowee Governors Cold Start	1.55E-5	23	CC	• HGT TUR 1,2/CS	1.62E-5
20	CC	• Governor Oil Systems - Run	1.40E-5	24	CC	• KU1,KU2 Oil and Air Systems	1.46E-5

CC: Common cause failure

Ind: Independent random failure

Table A-1. Top 20 cutsets of the Fault Tree and REVEAL\_W™ models<sup>2</sup>

### A.2.2 Independent Estimate of Keowee Failure Probability

Without recoveries, the probability of Keowee failing to supply Oconee with emergency power was estimated to be 0.010 using the Duke Fault Tree model.

The REVEAL\_W™ model was constructed so that different configurations could be run separately. Each configuration has dramatically different cutsets. Running the configurations separately and combining them using conditional probabilities permitted independent estimate of Keowee's failure probability. Moreover, it allowed a look at the different modes of failure: That is, the common cause failures when both units were running and the independent single cause failures when one unit was in maintenance.

<sup>2</sup> The cutset "All Keowee Aux Power Breakers Fail" is not produced because REVEAL\_W™ models common cause failures differently.

Four possible states must be combined:

**K1SUK2SO:** KU 1 Standby, Aligned Underground, KU 2 Standby, Aligned Overhead.

**K1SUK2GO:** KU 1 Standby, Aligned Underground, KU 2 Generating to Grid, Aligned Overhead.

**K1SUK2M:** KU 1 Standby, Aligned Underground, KU 2 in Maintenance.

**K1MK2M:** KU 1 in Maintenance, KU 2 in Maintenance.

Table A-2 lists each of the four states, the probability of being in each state (using draft PRA data), and the corresponding probability of failure generated from the REVEAL\_W™ model. The independently generated 0.010 duplicates the Fault Tree model's 0.010. To substantiate each component of this final value, the top cutsets of each portion are set out in Tables A-3 through A-5, below.

STATE (Configuration)	Fraction of Time Keowee in State	Conditional Probability of State	Failure Probability
K1SUK2SO	9.32E-1	3.93E-3	0.00366
K1SUK2GO	2.44E-2	3.76E-3	0.00009
K1SUK2M	3.8E-2	3.03E-2	0.00115
K1MK2M	5.23E-3	1.00E+0	0.00523
Total Probability:			0.0101

Table A-2. Conditional probabilities of Keowee: REVEAL\_W™ model

Table A-3. Cutsets from K1SUK2SO

#	Type	Description	Comment
1	CC	• Both Unit's WL Filters Clogged	Neither Unit is Cooled; Neither Can Run
2	CC	• Failure of The Excitation Breakers	Neither Unit Will Run
3	CC	• Excitation:Base Adjust Fails	Neither Turbine Will Run: Excitation
4	CC	• Both Turbines Fail to Run	Neither Turbine Will Run
5	CC	• DC Batteries Fail	Neither Unit Can Cold Start or Hot Start
6	CC	• CWS Control Valves Fail	Neither Unit is Cooled; Neither Can Run
7	CC	• AC Xfmrs CX,1X,2X Fail	AC Power Lost; Neither Unit Can Run
8	CC	• Battery Chargers Fail	Neither Unit Can Cold Start or Hot Start
9	CC	• Governors Fail to Run	Governors Fail; Neither Unit Will Run
10	CC	• Governor Air Systems	Governors Fail; Neither Unit Will Run
11	Ind Ind	• Excitation Base Adjust Fails U1 • Excitation Base Adjust Fails U2	Excitation Fails; Units Will Not Run
12	Ind Ind	• GBOHX: Latent Human Error • Excitation Base Adjust Fails U2	Guide Bearing Oil System Fails Unit 1 Discontinued Excitation Fails Unit 2
13	Ind Ind	• GBOHX: Latent Human Error • Excitation Voltage Adjust Fails U2	Guide Bearing Oil System Fails Unit 1 Discontinued Excitation Fails Unit 2
14	Ind Ind	• Excitation Voltage Adjust Fails U2 • Excitation Base Adjust Fails U1	Neither Unit is Excited; Both Will Not Run
15	Ind Ind	• Excitation Voltage Adjust Fails U1 • Excitation Base Adjust Fails U2	Neither Unit is Excited; Both Will Not Run
16	Ind Ind	• GBOHX: Latent Human Error • Unit 2 Generator Fails To Run	Guide Bearing Oil System Fails Unit 1 Unit 2 Fails to Run
17	Ind Ind	• Excitation Base Adjust Fails U2 • Unit 1 Generator Fails To Run	Unit 2 Excitation Fails Unit 1 Fails to Run
18	Ind Ind	• Excitation Base Adjust Fails U1 • Unit 2 Generator Fails To Run	Unit 1 Excitation Fails Unit 2 Fails to Run
19	Ind Ind	• Excitation Voltage Adjust Fails U1 • Excitation Voltage Adjust Fails U2	Unit 1 Excitation Fails Unit 2 Excitation Fails
20	CC	• Emergency Start Signals	Neither Unit Will Start

Table A-4. Cutsets from K1SUK2GO

#	Type	Description	Comment
1	CC	• Both Units' WL Filters Clogged	Neither Unit is Cooled; Neither Can Run
2	CC	• Failure of The Excitation Breakers	Neither Unit Will Run
3	CC	• Both Turbines Fail to Run	Neither Turbine Will Run
4	CC	• DC Batteries Fail	Neither Unit Can Cold Start or Hot Start
5	CC	• CWS Control Valves Fail	Neither Unit is Cooled; Neither Can Run
6	CC	• AC Xfmrs CX,1X,2X Fail	AC Power Lost; Neither Unit Can Run
7	CC	• Battery Chargers Fail	Neither Unit Can Cold Start or Hot Start
8	CC	• Governor Air Systems	Governors Fail; Neither Unit Will Run
9	Ind Ind	• GBOHX: Latent Human Error • Excitation Voltage Adjust Fails U2	Guide Bearing Oil System Fails Unit 1 Discontinued Excitation Fails Unit 2
10	Ind Ind	• Excitation Voltage Adjust Fails U2 • Excitation Base Adjust Fails U1	Neither Unit is Excited; Both Will Not Run
11	Ind Ind	• Excitation Base Adjust Fails U1 • Unit 2 Generator Fails To Run	Unit 1 Excitation Fails Unit 2 Fails to Run
12	Ind Ind	• GBOHX: Latent Human Error • Unit 2 Generator Fails To Run	Guide Bearing Oil System Fails Unit 1 Unit 2 Fails to Run
13	Ind Ind	• Excitation Voltage Adjust Fails U1 • Excitation Voltage Adjust Fails U2	Neither Unit Will Run
14	CC	• Emergency Start Signals	Neither Unit Will Start
15	CC	• Generator Lockout Fails	Neither Unit Will Start
16	Ind Ind	• Excitation Voltage Adjust Fails U1 • Unit 2 Generator Fails To Run	Unit 1 Excitation Fails Unit 2 Fails to Run
17	Ind Ind	• Excitation Voltage Adjust Fails U2 • Unit 1 Generator Fails To Run	Unit 2 Excitation Fails Unit 1 Fails to Run
18	Ind Ind	• GBOHX: Latent Human Error • ACB 6 Fails to Close	Guide Bearing Oil System Fails Unit 1 Auxilliary Power Lost to Unit 2
19	Ind Ind	• Excitation Base Adjust Fails U1 • ACB 6 Fails to Close	Unit 1 Excitation Fails Auxilliary Power Lost to Unit 2
20	Ind Ind	• Unit 1 Generator Fails To Run • Unit 2 Generator Fails To Run	Neither Unit Will Run

Table A-5. Cutsets from K1SUK2M

#	Type	Description	Comment
1	Ind	• Excitation Base Adjust Fails U1	Unit 1 Excitation Fails; Will Not Run
2	Ind	• GBOHX: Latent Human Error	Guide Bearing Oil Fails; KU1 Will Not Run
3	Ind	• CWS Control Valve Fails	CWS Fails; KU1 Will Not Run
4	Ind	• Excitation Voltage Adjust Fails U1	Unit 1 Excitation Fails; Will Not Run
5	Ind	• Turbine Run Fails	KU1 Turbine Fails
6	Ind	• ACB 7 Fails to Close	Auxilliary Power Lost; KU1 Will Not Run
7	Ind	• Excitation Base Adjust Fails - Run	Unit 1 Excitation Fails; Will Not Run
8	Ind	• Governor Wicket Gates Fail	Governor Fails; KU1 Fails
9	Ind	• Governor Fails to Run	Governor Fails; KU1 Fails
10	Ind	• DC Battery Fails	DC Power Fails; KU1 Will Not Start
11	Ind	• Excitation Voltage Adjust Fails - Run	Unit 1 Excitation Fails; Will Not Run
12	Ind	• CWS - No Air Cooling	CWS Fails; KU1 Will Not Run
13	Ind	• Supply Excitation Breaker	Unit 1 Excitation Fails; Will Not Run
14	Ind	• Field Flashing Breaker	Unit 1 Excitation Fails; Will Not Run
15	Ind	• Generator Excitation	Unit 1 Excitation Fails; Will Not Run
16	Ind	• Field Breaker (Excitation)	Unit 1 Excitation Fails; Will Not Run
17	Ind	• CWS Control Valve	CWS Fails; KU1 Will Not Run
18	Ind	• Supply Breaker (Excitation)	Unit 1 Excitation Fails; Will Not Run
19	Ind	• Field Breaker (Excitation)	Unit 1 Excitation Fails; Will Not Run
20	Ind	• Governor Air System	Governor Fails; KU1 Will Not Run

### A.3 PERFORMING ADDITIONAL ANALYSES

#### A.3.1 Revisiting the Sensitivity Analyses in the Draft Report

One question that the Duke Power Company study proposed to answer is the effect of cycling one or both Keowee units to the grid, thus producing power while remaining available to Oconee as sources of emergency power. The draft report seems to answer this question by using the base case data obtained from the Fault Tree model. These data indicate that the grid-cycled unit is more reliable than the standby unit. Once this conclusion is accepted, sensitivity studies can be performed to determine the effect that individual model components have on overall Keowee reliability. However, this type of sensitivity analysis fails to address the question of grid cycling.

In the base case, Keowee Unit 2 generates to the grid a small percentage of the time (3%). Any failures resulting from this alignment would be subsumed as a small component of the overall failure and would marginally affect the failure probability of Keowee. Alternatively, the REVEAL\_W<sup>TM</sup> model was used to attempt to study the presence of grid cycling and its absence and compare the effects of each. Thus sensitivity studies were made of Keowee Unit 2 (1) when generating to the grid and (2) when in standby. The studies performed are similar to those described in Section 7.5, "Sensitivity Studies," in the Duke Power Company draft report.<sup>3</sup>

##### A.3.1.1 Generic versus Bayesian Updated Data

The Duke Power draft report states that a 50 to 80% increase in generic failure probability would have an effect that is "not large" on the Keowee failure probability, because "the KEOWTOP gate is largely dominated by the Keowee unit maintenance unavailability." (Section 7.5.1) The effect that such an increase would be expected to have on the relative reliability of grid cycling was not estimated.

Several runs were made using the REVEAL\_W<sup>TM</sup> model to illustrate the effects that generic data can have on the failure probability of certain intermediate gates. These analyses produced cutsets at a 1E-6 cutoff and were simply used as screening values.

To successfully provide power to Oconee, a Keowee unit must accomplish three things: (1) it must start (whether it performs a "hot start" or "cold start"), (2) it must run, and (3) it must transmit power along a tenable path to Oconee. In the base case, with Keowee Unit 1 in standby and aligned underground, and Keowee Unit 2 in standby and aligned to the overhead path, the following failure probabilities for Unit 2 were calculated as set out in Table A-6, below.

---

<sup>3</sup> The results of the SCIENTECH sensitivity analyses using the REVEAL\_W<sup>TM</sup> model are still preliminary.

**Table A-6. Probabilities of Keowee Unit 2 failing to supply Oconee**

Configuration	KU2 Start	KU2 Run	KU2 on Overhead Path	Overall: KU2 to Oconee
Unit 2 in standby for 30 days	1.35E-2	1.91E-2	8.55E-3	3.47E-2
Unit 2 generating to grid daily and in grid generation mode at the time of Emergency Start demand	1.09E-2	1.49E-2	8.55E-3	2.83E-2

The difference in failure probabilities between the two configurations (which indicates that generating to the grid does increase reliability) is primarily the result of using data that take credit for testing components daily when the unit cycles to the grid. The unit start, however, relies on many components, many of which are circuit breakers. A hot start (while generating to the grid) relies on circuit breakers more than a cold start does. The failure probabilities of many circuit breakers used in the model deviate significantly from their generic counterpart values. If generic values for circuit breakers are substituted into the model, the following failure probabilities result. (The percentile change follows each number.)

**Table A-7. Failure Probabilities of Keowee Unit 2 Supplying Oconee Using Generic Circuit Breaker Values**

Configuration	KU2 Start	KU2 Run	KU2 on Overhead Path	Overall: KU2 to Oconee
Unit 2 in standby for 30 days	1.73E-2 (28%)	1.92E-2 (1%)	8.55E-3 (0%)	3.86E-2 (11%)
Unit 2 generating to grid daily and in grid generation mode at the time of Emergency Start Demand	1.81E-2 (67%)	2.13E-2 (43%)	8.55E-3 (0%)	4.05E-2 (43%)

Table A-7 is illuminating in several respects. As noted in Duke's draft report, the effect of generic values may be "not large" on overall reliability, yet the values certainly affect the different alignments to different degrees. By way of illustration, only one of the many types of components was replaced here with generic values. The overall difference that generic data makes can potentially be much greater than the numbers shown in this table indicate.

**A.3.1.2 Grid Cycling versus Standby Unit Reliability**

The Duke Power draft report includes the following table<sup>4</sup>:

*Copied from report & report was in error*

**Table 3-4: Sensitivity Study Results:  
Grid Cycled Versus Standby Unit Reliability**

Failure Mode	Standby Unit Failure Probability	Grid Cycled Unit Failure Probability
Start Failure	1.6E-2	1.2E-2
Run Failure	9.2E-3	7.6E-3

*300*

From this table, "it is observed that the failure probabilities for the standby unit are slightly higher than for the grid cycled unit." (Section 7.5.2).

However, this conclusion is inaccurate on several points, the most important one perhaps being the failure to recognize that the requirements for the various starts on the underground and overhead paths are different. Table 3-4 illustrates the difference between "Standby: Underground," and "Grid-cycled: Overhead," which is certainly not the same as the distinction between "Standby" and "Grid Cycling." The difference stems from the fact that, when a unit is generating to the grid, the ACB dedicated to the overhead path for that unit is already closed. To regenerate to the overhead path, the ACB must be reopened, a lockout must occur, and then the ACB must be reclosed. If the unit is aligned to the underground path, however, the overhead ACB must open and the underground ACB must open and reclose, relying on a different series of signals with different failure probabilities. Thus "Grid Cycling: Overhead" is different from "Grid Cycling: Underground" and the fact should be recognized.

*→ were very sensitive to this*

Section 7.5.2 of the Duke Power draft report does not address any sensitivities of the Fault Tree model results but simply displays subsets of the results overall. As is shown later in this appendix, the conclusions arrived at from the overall Fault Tree results are eroded when certain sensitivity analyses are run.

*MISleading!*

**A.3.1.3 Recovered Versus Unrecovered Results**

The Duke Power draft report considers only the effects that recoveries have on the overall Keowee failure probability. The effects that recoveries have on each of the independent conclusions should be considered as well. Because the REVEAL\_W<sup>TM</sup> model was used for comparative purposes only, recovery events were not included in that model, either.

<sup>4</sup>It may be noticed that certain probabilities are significantly smaller than the probabilities produced in the REVEAL\_W<sup>TM</sup> model, especially considering that the latter model made use of a much higher cutoff value (1E-6 as opposed to 1E-8) than the Fault Tree model did when producing cutoff sets.

### A.3.1.4 Infrequently Tested/Demanded Components

The table used to observe the sensitivity of the system to infrequently demanded components shows three probabilities; (1) Unit 2 Startup, (2) Unit 2 Run, and (3) Overall Keowee Success.

Although it may be of interest to know what happens to KU2 when the reliability of infrequently demanded components changes, the change sheds no light on the reliability of the Standby and Grid-Cycling Units.

### A.3.1.5 Duke Power Company Sensitivity Study Conclusions

Overall, the sensitivity studies seem to suffer from the same problem as the cutset generation. The results are viewed in terms of Keowee reliability overall, and the interesting dynamics of the system are masked by the relative rigidity of this top node in the model. As mentioned in the Duke Power draft report, Keowee reliability is primarily a function of the amount of time that both units spend in maintenance. Most of the remaining failure probability results from the alignment when both units are in Standby. The importance of failures that are the result of KU2 generating to the grid is insignificant. Because their frequency is so small, they are reduced by two orders of magnitude.

The draft report states that the study of Keowee reliability as a source of emergency power for Oconee is being performed for several reasons. In Section 1.1 of the report, it is stated that what is wanted is "an analytical estimate of the reliability of Keowee to provide emergency power to Oconee." To a large extent, the structure of the analysis in all likelihood is a result of this limited objective.

*I wanted  
this  
taken  
out!*

The fourth and last objective of the study is to "derive insights on the adequacy and the value of the ongoing efforts to improve Keowee reliability." Authorization of different patterns of Keowee production to the grid is part of this effort, which is ongoing. Insights as to the adequacy and value of these efforts have not yet been provided. The following independent sensitivity analysis indicates the types of insights that might be helpful.

### A.3.2 SCIENTECH's Additional Sensitivity Analyses

The format of our independent sensitivity analysis was constructed to more accurately answer the questions posed in the Duke Power study. When performing the analysis, different cases will be run on the model, and these will be described briefly:

#### A.3.2.1 Number of Days Actually Generating to Grid

The data used in the Fault Tree model *assume* that when a unit is authorized for daily grid cycling it actually generates daily. This effectively "tests" many non-emergency components on a daily basis. Subsequently, the failure probability of many components is

*Averaging is not a good idea when looking at intervals*

SAFETY TECH, Inc

enough, even when authorized for daily cycling, a unit does not generate every day for a variety of reasons. This gives credit to the grid-cycling unit that is too generous and in our view is *not conservative*. Our examination of the operating data for the years 1993 and 1989 shows that a grid-cycled unit can go for many days without generating any power. It is expected that Duke will study the sensitivity of the final results to this nonconservative assumption (i.e., daily generation).

*possibly may revisit!*

**A.3.2.2 Bayesian versus Generic Data**

Generic data on individual component performance tend to indicate much lower reliability than do Bayesian updated data. Replacing the generic data with Bayesian updated data does not change the overall Keowee reliability appreciably but does however change the relative reliability of different Keowee configurations.

*check on this*

	Generic	Bayesian
Mechanical Opening or Closing of ACBs	1.2E-3	1.54E-4 - 7.04E-3 <sup>5</sup>
ACB Close Coil or Trip Coil	2.8E-3	2.9E-5

*need to find out where this came from*

**A.3.2.3 Independent Analysis**

*Davis Base*

The failure probability of each unit has to be addressed with respect to whether at the time of the emergency start demand the unit is in standby or is in grid-generation mode. Because of this, the failure probability of each Keowee Unit is generated according to three variables: (1) The number of days between generations or tests, (2) the data used, and (3) the nature of the configuration at the time of emergency start demand. These numbers are shown in the following two tables.

Table A-8. Sensitivity values for Keowee Unit 1

Days between Grid Generations or Test	Circuit Breaker Data	Configuration at the time of Emergency Start Demand	Unit Start	Unit Run	Pathway	Overall
1	Bayesian	Standby	8.05E-3	1.76E-2	1.31E-3	2.64E-2
1	Bayesian	Grid	1.67E-2	1.76E-2	1.31E-3	3.53E-2
30	Bayesian	Standby	9.63E-3	2.12E-2	1.31E-3	3.13E-2
1	Generic	Standby	8.05E-3	1.77E-2	1.31E-3	2.65E-2
1	Generic	Grid	1.77E-2	1.77E-2	1.31E-3	3.67E-2
30	Generic	Standby	9.36E-3	2.13E-2	1.31E-3	3.14E-2

*Mike Barrett is concerned about this - his model only shows ~ 5% difference*

<sup>5</sup> In this case, the two ACBs that facilitate grid generation have a lower failure probability than the generic value, while the two that do not facilitate grid generation have a higher failure probability. Small inconsistencies such as this one indicate that Keowee Unit 2 (generating to the grid and aligned to the overhead path) is more reliable than Keowee Unit 1. Considering the method of calculating Bayesian probabilities, this certainly is not surprising. Every time Unit 2 generates to the grid, it establishes a history. The underground ACBs (and Unit 1) have not had the opportunity to establish this history.

Table A-9. Sensitivity Values for Keowee Unit 2

Days between Grid Generations or Test	Circuit Breaker Data	Configuration at the time of Emergency Start Demand	Unit Start	Unit Run	Pathway	Overall
1	Bayesian	Standby	1.20E-2	1.49E-2	8.55E-3	2.90E-2
1	Bayesian	Grid	1.09E-2	1.49E-2	8.55E-3	2.83E-2
30	Bayesian	Standby	1.35E-2	1.91E-2	8.55E-3	3.47E-2
1	Generic	Standby	9.36E-3	2.13E-2	8.55E-3	3.14E-2
1	Generic	Grid	1.81E-2	2.13E-2	8.55E-3	4.05E-2
30	Generic	Standby	1.73E-2	1.92E-2	8.55E-3	3.86E-2

The failure probability of Keowee Unit 1 when it is in standby and has not been tested or used for grid generation for 30 days is  $3.13E-2$ , using the Bayesian values suggested for the Fault Tree model. The failure probability of this unit while it is generating to the grid at the time of the emergency start is  $3.53E-2$ . The *nonconservative assumption* is that Unit 1 has generated to the unit in the last 24 hours. That is, credit is taken for daily testing of many components. Often, the unit does not generate to the grid on a daily cycle; because of limitations such as water availability, the time between generations can be many days.

## A.4 CONCLUSIONS

### A.4.1 Conclusions in Chapter Seven of the Duke Power Draft Report

Certain conclusions stated in Section 7.6 of the Duke Power draft report are discussed in light of the independent sensitivity analysis conducted thereafter using the REVEAL\_W™ model.

#### A.4.1 Keowee Unit Reliability

In Conclusion 3 of the Duke Power draft report the excitation system is cited as the main source of unit failure. It is true that this system is a main source of unit failure. However, an equally important source of failure is the circuit breakers that allow cold and hot starts for each unit. The reliability of each unit's start sequence is highly sensitive to the reliability values attributed to each ACB and PCB.

#### A.4.1.2 Use of Keowee for Grid Generation

In Conclusion 1 it is claimed that the grid-cycling unit is more reliable than the standby unit. This claim is challenged by the preliminary results of the independent sensitivity analysis conducted subsequent to the Duke Power draft report.

Conclusion 2 states that Keowee Unit 2 "may be started almost daily." What do the qualifiers "may" and "almost" mean? KU2 is taking credit for daily generation of components that erode over time.

### A.4.2 Conclusions Arrived at Using the REVEAL\_W™ Keowee Model

Far from exhaustive, the sensitivity analyses performed using the REVEAL\_W™ model merely indicate the direction that the Duke Power Fault Tree model sensitivity analysis should have taken. The main conclusions that resulted from using the REVEAL\_W™ model are as follows:

- The circuit breakers and associated relays are critical components when differentiating between hot and cold starts. The method of starting a unit is the fundamental difference between a unit in standby mode and a unit cycling to the grid.
- Viewing different configurations in isolation is essential in understanding their dominant failure modes and in determining how they each affect the overall system differently.

- Maintenance of the Keowee Units accounts for about half of the overall Keowee failure probability. Time in maintenance is not a function of system configuration, however. It is a factor that should remain external to analyses made to compare the reliabilities of different system configurations.

## A.5 REFERENCES

1. "Oconee Nuclear Station Keowee Reliability Analysis." Draft Report, Duke Power Company, December 1994.
2. "REVEAL\_W<sup>TM</sup>, A Modularized Safety & Reliability Analysis System for Windows," SCIENTECH, Inc., 1994.

**APPENDIX B**  
**Letter re High-Level Review Comments on the**  
**Keowee PRA**

SCIENTECH, Inc.  
March 1995

March 30, 1995

Dr. Homayoon Dezfuli, PhD.  
SCIENTECH, Inc.  
11140 Rockville Pike, Suite 500  
Rockville, MD 20852

Subject: High Level Review Comments on the Keowee PRA

Dear Dr. Dezfuli:

Per your request I have conducted a limited high level review of the subject Keowee PRA effort based on my past experience in conducting full PRAs which have done detailed modelling of the onsite power systems of plants on multi-unit sites.

As I understand, the licensee has submitted the Keowee PRA report to NRC to begin a dialogue regarding the reliability of the onsite power system in various modes of operation. They would eventually like to obtain approval from NRC for running both of the Keowee Hydroelectric dams for commercial power generation in addition to their emergency role for supplying power to the onsite electric system following loss of offsite events and design basis accidents. The PRA models contained in the report address supplying power from Keowee to Oconee Unit 3 (which was the subject of a major PRA in it's own right).

As a high level review comment, the existing scope of the analysis is currently too narrowed to shed light on the obvious safety issues involved in the current and proposed modes of the operation of the onsite electric system. The consideration of interactions from Oconee Units 1 and 2 on the reliable delivery of emergency power to Unit 3 was beyond the scope of work as defined in Section 4.2 of the report. This renders the PRA models not being able to address the issues of the likelihood and consequences of electrical systems interactions between the various Oconee units and the two Keowee units. The conclusions reached about the overall reliability of the onsite power system in the Executive Summary in Section ES 4.2 are thus beyond what was actually analyzed.

One of the ways an emergency bus could be lost is via an uncleared fault from an emergency load, or a breaker that does not open and reclose in the proper timeframes. This is a consideration for Unit 3. If the potential effects of such faults originating from Units 1 or 2 are additionally considered on the reliability of the main buses to deliver power to any unit, one would find 3x

the potential for such effects over what was actually modelled. Additionally, three nuclear power plants are effected, not one. If these items were taken into consideration, it is possible that different conclusions might be reached. As a followup effort, I would recommend that this issue be pursued and the PRA model upgraded.

I additionally found some other items, which while of less significance to the overall results, are also provided for your consideration. The Bayesian update process as documented in Table 5.3-1 appears to have some mathematical problems. I can only assume the work utilized a procedure or computer code without sitting back and asking if the results made any sense. I have performed Bayesian updates of reliability data in numerous PRA studies to incorporate new experience. It should not be possible to lower a mean failure rate via a Bayesian update, by incorporating a relatively small amount of new experience, while preserving the same error factor. This is because the new information is too limited to overwhelm the prior distribution.

As an example: circuit breakers failing to close starts with a prior distribution mean of  $1.2E-03$ . The new experience cited amounts to 222 demands. Given 222 demands the expected number of failures would be 0.26, implying one would need roughly four times that many demands to see another failure. Somehow the Bayesian update resulted in a 25% reduction in the failure rate. This makes no sense, because the additional experience should not be able to overwhelm the prior distribution.

As another example: spurious operation of a solenoid valve starts out with a prior distribution mean value of  $4.1E-07$ /hr. The new experience amounts to 171,412 hours which initially sounds appreciable. The expected number of failures for this experience, however, would only be 0.07. To lower the prior mean one would thus need more than 15x as much experience without any failures. The Keowee PRA somehow reports an updated mean which is 5% lower, and again with no change in the error factor. I cannot tell what was done wrong without seeing the details of the licensee's calculations but there is clearly something wrong in the way these calculations were performed. If you were interested, I could redo all of these updates.

An item I am unclear on relates to the modelling of the relay logic (undervoltage, underfrequency, close, generator lockout, and trip etc.). I would normally expect to see considerable logic loops and interconnections in this logic than I found when I reviewed Appendix A. This is due to the set/reset relay logic normally used to control breakers. How this was simplified to produce the fault trees is unclear to me. Pursuing this would require access to the actual control relay diagrams and one-line drawings.

Another item which needs clarification is the thoroughness of the electrical logic testing. In the fault summary tables various references are made to the

types of test programs utilized. The testing uses the term "functional testing". In cases where redundant logic is utilized it is unclear to me if the testing program confirms operability of individual redundant portions of the logic or is simply an integrated logic test that confirms that at least one portion of the logic is operable. This impacts the reliability dramatically and needs to be confirmed. \*

If there are any items requiring further review, please feel free to contact me.

Sincerely,

Signature on file

Dr. John H. Bickel  
Sr. Project Manager

**APPENDIX C**  
**Comments on the HRA Part**  
**of the Keowee PRA Study**  
**(Draft Report, December 1994)**

SCIENTECH, Inc.  
March 1995

## APPENDIX C

Comments on the HRA Part of the Keowee PRA Study  
(Draft Report, December 1994)

pp. C.3-8 to C.3-12

The quantification of latent and recovery actions are performed using generic data from NUREG/CR-1278, NUREG/CR-4772, and EPRI-TR-100259. Are there any Keowee-specific human reliability data that can be used to either directly estimate the human error probabilities (HEPs) or supplement the generic values in the above reports (given a significant amount of Keowee-specific equipment reliability data exist)? The report states that a review of the Keowee and industry operating history in the context of human reliability was conducted by the HRA team (p. C.3-3). However, please clarify if any data obtained from the review was used in the process of quantification of human error probabilities.

Particularly, Keowee-specific data for latent human errors such as FK1GBHXLHE (see Table 7.2-4) and EK2BASELHE (see Table 7.2-5) which are among the top five significant contributors to the unreliability of the underground and overhead units, respectively, are essential for their quantification.

pp. C.3-20 to C.3-26 (Enclosure C.3-1)

In the process of quantification of the latent human errors for Unit 1 and Unit 2, sometimes credit is given to operability tests for Unit 2 (see assumptions 3 and 4 on Page 4-6). This assumption is not consistently applied to all latent human errors. Why?

For example, credit for operability test is given to human errors FK2120GLHE and FK2GBHXLHE for the overhead unit (see Table 5.5-1) which resulted in an HEP estimate of  $2.6E-04$ , whereas such a credit is not given to human errors EK2BASELHE, BK2GBDCLHE, PK2TSDCLHE, OK2002BLHE, or OK2002CLHE for the overhead unit which resulted in an HEP estimate of  $3.2E-03$ . Is it true to say that the equipment in the latter group are not called upon to operate during the daily grid generation function?

p. C.3-22; EK1BASELHE and EK2BASELHE

Figures C.3-1, C.3-2 and C.3-3 are established for proceduralized maintenance activities and the probabilities taken from NUREG/CR-1278 and NUREG/CR-4772 to qualify these event trees also apply to proceduralized actions. In the Keowee report (p. C.3-23) it is stated that there is no established procedures for making the base voltage adjustment, however if needed, a "special procedure" would have to be written. Figure C.3-2 was used to quantify this human error. The applicability of this event tree and its probabilities to this maintenance activity is questionable.

Furthermore, the probability estimates used to quantify these event trees have the implicit assumption that the personnel are trained on the use of procedures. It is not clear if the Keowee personnel have training on these "special procedures".

What are the bases and justification for using Figure C.3-2 to quantify EK1BASELHE and EK2BASELHE ?

p. C.3-11, Section C.3.3.6.4

**Time sensitivity of recovery actions**

The decision tree model in EPRI-TR-100259 is used in Keowee PRA to quantify recovery actions. The time reliability model is not used in the study. It is noted that the decision tree approach in the EPRI-TR-100259 complements the time reliability method. For time-sensitive actions, the HEP can be dominated by the operator non-response in a timely manner which is usually quantified by using time reliability correlations (TRCs). An example is recovery action AB0SWGRREC where the time available and time taken to perform the action are comparable (about one hour).

Therefore, it is important to examine the time sensitivity of the recovery actions (i.e., comparing the time available versus time taken to identify and execute the recovery action) before using the decision tree model.

Did the HRA team consider the time sensitivity of all the recovery actions modeled in the Keowee PRA? In particular, what are the time available and the time taken to identify and execute the recovery actions ABEOPRCREC (p. C.3-28) and ABPOPRCREC (p. C.3-29)?

For recovery actions FK0FISHREC (p. C.3-31) and GK0BRGVREC (p. C.3-33), it is stated that there is ample time available to complete the actions. What are the available times and the response times for these recovery actions?

**Action phase of recovery actions**

A value of 0.05 is used for the failure to perform the recovery action once it has been identified by the control room operator. The bases for using this value are not stated in the Keowee study, however, it seems a reasonable estimate. There are two issues with regard to its implementation in the study.

1. The contribution from the action phase is only used for recovery actions that are performed from the outside of the control room (it has been assumed that this contribution is negligible for actions inside the control room). This assumption can be valid when the actions from the control rooms are few, simple, and well practiced and trained on. The NUREG/CR-4772 (Table 8-5) provides a range of 0.02 to 0.25 for the HEP to perform a critical proceduralized action from the control room.

Did the HRA team consider the validity of this assumption for all the control room-based recovery actions modeled in the Keowee PRA? In particular, the 9.0E-03 estimate for recovery actions ABEOPRCREC (p. C.3-28) and ABPOPRCREC (p. C.3-29)

seem to be low. Are these recovery actions simple, proceduralized, and well trained by the control room operators?

2. A single value of 0.05 has been used for the action phase of the recovery actions to be performed from the outside of the control room. This value can be an underestimate depending on the nature of the task to be performed. **The overall HEP for the action phase depends on the number of actions to be performed, their complexity, the quality of the procedure (if any), and the level of practice/training of the personnel.** For complex recovery actions, human reliability event trees (NUREG/CR-1278 and NUREG/CR-4772) or human reliability fault trees (EPRI-TR-100259) are usually used to model the action phase.

Are all the modeled recovery actions simple from the execution point of view, proceduralized, and trained on so that a single value of 0.05 can be used in every case? Please justify the rationale behind using 0.05 for recovery action for FKOFISHREC.

**APPENDIX D**  
**Comments on the Data Analysis/Results of**  
**the Keowee PRA Study**  
**(Draft Report, December 1994)**

## APPENDIX D

**Comments on the Data Analysis/Results of the Keowee PRA Study  
(Draft Report, December 1994)**

## D.1 Summary

A review is performed of the Keowee probabilistic risk assessment (PRA) documented in Ref. 1. Although some of the specific suggestions in prior reviews (Refs. 2 and 3) of the Keowee reliability database have been incorporated into Ref. 1, Ref. 1 has not resolved the basic concerns underlying the three fundamental recommendations in Ref. 2. Consequently, there is some remaining uncertainty regarding the validity of the Ref. 1 results.

Comparing the reliability of Keowee with the reliability of more conventional emergency power sources discloses that their failure probabilities are similar. Because of residual uncertainties regarding the Keowee PRA database, there is a concern that the actual Keowee reliability may be lower than predicted. However, information in Ref. 1 indicates that the Lee station reliability may be 95% or greater (given that other sources of offsite power are lost and both Keowee units are unavailable).

It is recommended that the reliability improvement in emergency power afforded by the Lee station be more rigorously quantified. In the absence of a defensible reliability value for Lee station, the PRA should apply a more conservative and screening-type reliability value. If a more rigorous quantification cannot confirm a reasonable reliability for the Lee station (e.g., at least 95%), consideration should be given to ensuring adequate emergency power availability by revising the Oconee Technical Specifications to limit the amount of time the Oconee units can operate when both Keowee units are unavailable.

Use  
this  
in  
Final

## D.2 Introduction

A critique is performed of Ref. 1, predicated in part on prior reviews (Refs. 2 and 3) of the Keowee reliability assessment database. Specific review comments are presented in Section 3. Section 4 contains general conclusions and recommendations.

## D.3 Keowee PRA Review

The Ref. 1 response to comments from Refs. 2 and 3 is addressed in Section 3.1. Section 3.2 provides a general review of the Ref. 1 PRA.

### D.3.1 Response to Prior Review Comments

Reference 2 includes three fundamental recommendations for enhancing the Keowee reliability assessment database:

1. define the nomenclature (including statistically precise definitions where appropriate);
2. include comparisons of Keowee data with other recognized data sources and rationalize any discrepancies; and
3. add a good methodology description with a rationale for its selection.

Reference 2 also contains several specific suggestions for enhancing the Keowee reliability assessment database. Although some of the specific suggestions in Ref. 2 have been incorporated into Ref. 1, Ref. 1 has not resolved the basic concerns underlying the three fundamental recommendations.

Two basic concerns underlie the fundamental recommendations in Ref. 2. As discussed in Ref. 3, these concerns are:

1. the applicability of generic nuclear power data to a hydroelectric plant; and
2. uncertainty regarding the specific techniques and data used to develop the Keowee reliability assessment database.

The applicability of the generic data to a hydroelectric plant is addressed by Recommendation 2. Recommendations 1 and 3 pertain to the second concern.

### D.3.2 General Review of the Keowee PRA

The general review of Ref. 1 focuses on a single topic - whether the unique emergency power supply for the three Oconee nuclear generating units has reliability characteristics comparable to the more conventional emergency power supplies encountered in other nuclear power plants.

#### D.3.2.1 Potential Impact of the Keowee PRA on Oconee Technical Specifications

Diesel generators are the more conventional emergency power supplies typically used in nuclear power plants. If the two Keowee units are compared

to two diesel generators, similar failure probabilities result. According to Ref. 1, the overall Keowee unavailability is 0.0071. Using generic data from Ref. 4 for diesel generators, the probability that two, 100% capacity diesel generators fail to perform their mission is 0.0069. Clearly, this is a negligible difference. However, a major dissimilarity between Keowee and conventional emergency power supplies is the cause for their respective failure probabilities. 

The failure probability analysis for two, 100% capacity diesel generators considered two system states:

1. both diesel generators initially available; and
2. only one diesel generator initially available (the other being unavailable due to maintenance).

Given that both diesel generators are initially available, system failure can only occur if:

- both diesel generators fail to start;
- one diesel generator fails to start and the other starts but fails to operate the required mission time; or
- both diesel generators start but fail to operate the required mission time.

Given that only one diesel generator is initially available, system failure can only occur if the available diesel generator:

- fails to start; or
- starts but fails to operate the required mission time.

Two simplifications are inherent in the diesel generator failure model:

1. recovery is ignored (which is conservative); and
2. the system state where both diesel generators are initially unavailable (due to maintenance) is omitted.

Omitting the system state where both diesel generators are initially unavailable is standard in PRAs because Technical Specifications generally prohibit a nuclear plant from operating at power if its emergency power system is unavailable. Hence, the probability of the plant experiencing this system state is low. However, Ref. 1 indicates that the main contributor to the

overall Keowee unavailability is the unavailability of both units due to maintenance. According to Ref. 1, the probability of this system state is 0.005, just over 70% of the overall Keowee unavailability. Therefore, a salient issue regarding whether the Keowee units have reliability characteristics comparable to the more conventional emergency power supplies encountered in other nuclear power plants is whether enhanced assurance of emergency power availability could be gained by imposing more conventional Technical Specifications.

Enhanced assurance of emergency power availability is potentially important for Oconee because of uncertainties in the Keowee PRA results. Although Figure 7.5-1 in Ref. 1 indicates that the ratio of the 95<sup>th</sup> quantile to the median is just over two, this result is apparently predicated solely on uncertainties in the input data. Since the basic concerns underlying the Keowee database have not yet been resolved, there may be greater uncertainty in the Keowee unavailability assessment than Ref. 1 credits. Assurance that these unquantified sources of uncertainty do not render the actual Keowee unavailability significantly greater than the unavailability of more conventional emergency power sources could be achieved by imposing more conventional Technical Specifications that would essentially eliminate the dominant contributor to emergency AC unavailability.

#### D.3.2.2 Potential Impact of the Lee Generating Station on Emergency Power Availability

Keowee is not the only source of emergency power available to the Oconee units. Although it is the preferred source of emergency power, the three unit Lee combustion turbine station can be used to energize the Oconee ac power system. Thus, this additional source of emergency power affords some compensation for uncertainties in the Keowee reliability relative to more conventional sources.

Using the Lee station to energize the Oconee ac power system requires that:

- the Lee station be available; and
- operators in the control room manually close the SL breakers.

If the Lee station is initially unavailable, 30 to 60 minutes are necessary to bring it on-line and dedicate it to Oconee. This is insufficient time to prevent core damage immediately after a loss of offsite power unless the ac independent turbine driven emergency feedwater pump furnishes core cooling. Reference 1 implies that the probability the turbine driven emergency feedwater pump fails is approximately 0.017. This suggests that even if both Keowee units and the Lee station are not immediately available, there may be sufficient time to bring Lee on-line and dedicate it to Oconee.

Three conditions are necessary before the Lee station can provide power to Oconee.

1. The Lee station must be operational. If all three of its units are unavailable, it must be started and brought on-line before core damage occurs.
2. The transmission lines linking Lee with Oconee must be operational. Since these lines are not rugged against severe weather, there is a potentially high conditional probability that any loss of offsite power due to severe weather conditions will also sever the link between Lee and Oconee.
3. Oconee control room operators must manually close the SL breakers.

Availability data for the Lee station are not readily evident in Ref. 1. However, since the turbine driven emergency feedwater pump allows time for the Lee station to be started, the likelihood that power at the Lee station can be made available before core damage occurs should be high.

Reference 1 tabulates the probability that Oconee control room operators fail to manually close the SL breakers as 0.01 or 0.05, depending on the specific conditions involved. Also, Ref. 1 gives  $2.23 \times 10^{-3}$  and  $7.80 \times 10^{-3}$  as the respective probabilities that Lee fails to operate for the required mission time and that the transmission line from Lee fails. Combining these data with the supposition that Lee can be made available in an emergency with high probability, the probability that the Lee station fails to provide emergency power is in the range: 0.02 to 0.06.

#### D.4 Conclusions and Recommendations

Main conclusion that emerges from the Section 3 review

Although some of the specific suggestions in prior reviews (Refs. 2 and 3) of the Keowee reliability assessment have been incorporated into Ref. 1, Ref. 1 has not resolved the basic concerns underlying the three fundamental recommendations. These concerns are:

- the applicability of generic nuclear power data to a hydroelectric plant; and
- uncertainty regarding the specific techniques and data used to develop the Keowee reliability assessment database.

Consequently, there is some remaining uncertainty regarding the validity of the Ref. 1 results.

Comparing the reliability of Keowee with the reliability of two diesel generators (which represent more conventional emergency power sources) discloses that their failure probabilities are similar. However, the overall unavailability of Keowee is dominated by the situation where both units are unavailable due to maintenance. Because of residual uncertainties regarding the Keowee PRA database, there is a concern that hardware failures and operator errors may be more significant than evaluated. Combining this with the already high maintenance unavailability suggests that the actual Keowee reliability may be lower than predicted.

Information in Ref. 1 indicates that the Lee station reliability may be 95% or greater (given that other sources of offsite power are lost and both Keowee units are unavailable). It is recommended that the reliability improvement in emergency power afforded by the Lee station be more rigorously quantified. If a more rigorous quantification cannot confirm a reasonable reliability for the Lee station (e.g., at least 95%), consideration should be given to ensuring adequate emergency power availability by revising the Oconee Technical Specifications to limit the amount of time the Oconee units can operate when both Keowee units are unavailable.

#### D.5 References

1. "Oconee Nuclear Station Keowee PRA," Draft, Duke Power Company, December 1994.
2. Everline, C. J., "Keowee Reliability Database Review," Rev. 1, November 1994.
3. Keowee PRA Review Teleconference, January 26, 1995.
4. "Individual Plant Examination for the Davis-Besse Nuclear Power Station," Toledo Electric Co., 1993.

#### 4.0 METHOD of ANALYSIS

##### 4.1 AC Motor Operated Valves

###### A. ASDOP Input Data

The ASDOP file is created by modifying the base file ON2LCA00 from calculation OSC-4442. This file, ON2LCA00, was edited to add some 208 volt busses and their associated 600/208V transformer and each GL 89-10 AC MOV. A constant static load equivalent to half its associated 600/208V transformer rating is assumed on each 208V bus modeled. Overload heater resistances were modeled for each GL 89-10 MOV. Appendix 2 shows the overload heater sizes for each applicable MOV and Attachment 1 contains the overload heater resistance values. Appendix 1 shows a single line representation of what is modeled in this calculation. The changes and additions to the base file can be seen in Appendix 3. The new created ASDOP file is kept as DK73.PERASDOP(ON2MOV00).

The table in Appendix 2 shows MCC and compartment No., MOV data, and overload heater data. MOV data was obtained from actual test, MOV nameplates, and from valve manufacturer produced tables and curves. The valve MCC data and overload heater data was obtained from Duke single line drawings and manufacturers MCC drawings. Cable lengths were obtained from Duke outline drawings, cable sheets and plant walkdowns. This data can be seen in Appendix 2.

###### B. ASDOP Cases

This calculation analyzes the Unit 2 Auxiliary Power System under LOCA conditions with normal loads running and the 230KV switchyard supplying power through the start-up transformers. The 230KV switchyard is assumed to be at its minimum value. This calculation assumes that upon ES actuation the ES MOVs will stall until the 4KV and 575V motors accelerate to rated speed. Calculation OSC-2060 further explains this assumption. Also, reference calculation OSC-1612 page 29. This calculation also assumes that only one MOV which receive an ES signal and is normally in its ES position has to start during an ES event. (i.e. All normally ES positioned MOVs are in their ES position except for one during an event. Each MOV is analyzed to determine the worse case voltage.)

The manually initiated MOVs are started after the ES MOVs have completed their cycle. These valves are assumed to be started one at a time.

The following is a list of ASDOP cases performed for this calculation.

#### 4.0 CONCLUSION AND RECOMMENDATION

Based on the results and analyses given in Sections 7, 8, and Appendix B, it can be concluded that Oconee Unit 2 Auxiliary Power Systems are adequate for all modes of operation as described in the purpose and scope statement of this calculation. However, the following minor points need to be brought out.

1. Under a LOCA condition, during the initial start, some of the motor-operated valves (MOV's) may stall for up to 6 seconds because their terminal voltages are below the 80% criteria. However, the valve motors actually start unloaded within a few cycles. They will receive a load current less than the modelled locked-rotor amps (either rated-torque amps or average-load amps) after that brief starting period. Additional study on the MOV's is given in OSC-4582.
2. It is optimal to keep the generator bus voltage at or below 18.9 KV to avoid any overvoltage on the 6.9 KV system. Based on 1992 hourly Operator Aided Computer (OAC) data samples, the generator is at or below this value for the majority of the time during which Unit 2 is on-line. Furthermore, the OAC readings show that the generator voltage does not exceed 19.15 KV for 95% of the on-line time. The corresponding ASDOP case indicates no significant 6.9 KV overvoltages with the generator voltage at 19.15KV. Therefore, no additional corrective action is required to maintain the generator bus voltage below 19.15 KV since that value is only rarely and intermittently exceeded.
3. A short period of degraded grid condition is acceptable. A tech spec (3.7) change has been proposed to insure that the degraded grid condition would not remain for a long period of time.
4. Considering over-voltage contingencies and the zero-impedance bolted three-phase fault, the calculated short-circuit interrupting rating for the worst-case 4.16 KV switchgear (particularly the minimally loaded feeders from 2TC) has essentially no margin for the Normal Operation mode. However, the contribution through the incoming breaker is well within the rating. Close-and-latch ratings are not exceeded, but are similarly marginal for the Normal Operation and LOCA modes. Additional close-and-latch margin is provided by the higher tested rating.
5. Calculated fault currents exceed the rating of the 6.9 KV switchgear for a fault that occurs within the switchgear. However, since the switchgear is metal-clad and the feeder cables are all interlocked armor, the possibility of having a fault within the switchgear or on the cables is very remote. For all modes of operation, a fault at the loads will not produce a fault current exceeding the switchgear rating. The breakers will interrupt the fault at the loads as designed. The only possibility that a fault may occur within the switchgear is during maintenance. In this mode, there should not be any motors connected to the bus. Without contribution from the motors, fault current will not exceed the rating of the switchgear. (See the Shutdown case). Another type of fault that may occur is a high impedance arcing fault. As its name indicates, this type of fault will introduce a very high impedance to the circuit and the resulting fault current will be low. Based on this observation, it is concluded that the 6.9 KV switchgear is adequately operable.



# Oconee Nuclear Station

## Problem Investigation Process

### Problem Investigation Form

PIP Serial No: 4-095-1686  
MSE Serial No:

LER Serial No:  
Other Report:

to verify the Keowee units will start and carry the emergency loads for a specified time was not observed.

The Keowee test procedures reviewed did not specify a minimum unit run time to allow a correlation between the design basis run time of seven days and support system requirements nor was there documented justification for not performing the testing. Several other design basis calculations have not been proven by the test procedures to date. For example:

- Turbine Guide Bearing Oil Reservoir level control greater than 4.5 inches
- Turbine Guide Bearing Oil temperature control at 167 degrees
- Air Circuit Breaker supply air reservoir minimum pressure
- Lower Oil Reservoir temperature control greater than 80 degrees
- Governor Oil Pressure Tank level and pressure at 62.47 inches and 350 psig
- Governor Oil sump temperature below 130 degrees
- Governor Oil Pressure Tank pressure and level
- Generator Air and Thrust Bearing temperature control
- Turbine Sump level control

2. An observation of the Testing Keowee Overhead ACBs TT/0/A/0610/11, was conducted. The purpose of testing was to gather information and data on the operation of the Keowee Air Circuit Breakers (ACB) when air supply is not available. Facts noted and observation included the following:

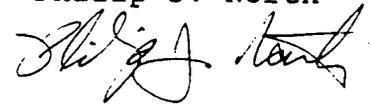
- The Design Basis of 145 psig minimum air reservoir pressure was not conclusively verified by the test method.
- An Oconee Control Room SRO was not notified by the test procedure steps.
- The approved test procedure results are documented by a calculation (OSC-5556). The calculation references and attaches a plant file memorandum, Addendum-4, Attachment-5.

In addition to the above concerns, the following memorandum statement highlights the test results versus the Design Basis:

"The 118# pressure switch, which had been set to trip the ACBs and clear the overhead power path, actuated during both the ACB1 and ACB2 140# tests, as evidenced by a computer point actuation. The pressure switch did not actuate during the 150# tests. Worst case past operability with the trip installed, assuming loss of the air supply system, and assuming 140# of air in the cylinder, the overhead ACB would not have closed due to the trip signal. With 150#, no air supply, and assuming 5#/hr leakage, the overhead path would have tripped within a couple of hours."

- a. As a result of the calculation, administrative controls or contingency plans are not in place to assure makeup air is available based on reservoir leakage or based on air compressor availability.
- b. The Design Basis of 145# air reservoir pressure baseline is questionable.
- c. Critical test results are documented in the memorandum. The calculation and results (memorandum) should be incorporated into an approved test procedure.

Prepared By: Philip J. North



Finding

SITA-92-01 (ON) (5:8-1)

Title: No single failure analysis for other than T=0.

Response:

- 1) Root cause for the finding: This SITA finding recommends that a single failure analysis of the electrical distribution system be performed for the worst case single failure, including those occurring after T=0, and ensure the system remains within design basis requirements. The finding is based on the auditors interpretation of the ONS design criteria, 10 CFR 50, Appendix K, and SECY 77-439.
- 2) Scope and results of the investigation performed to determine the extent of the finding: The attached memo confirms that Oconee is currently in compliance with licensing basis requirements.
- 3) Corrective steps which have been taken and the results achieved: Oconee is currently in compliance with licensing basis requirements, there corrective steps are not warranted.
- 4) Corrective steps which will be taken to avoid further findings: Oconee is currently in compliance with licensing basis requirements, there corrective steps are not warranted.
- 5) Date when full compliance will be achieved: Oconee is currently in compliance with requirements in the licensing basis.

January 12, 1992

MEMO TO FILE

Subject: Oconee Nuclear Station  
Single Failure Timing Licensing Basis

The single failure criterion is part of the Oconee licensing basis. The single failure criterion is a licensing review tool to assure reliable systems as one element of the defense in depth approach to reactor safety. In applying the criterion, it is not assumed that any conceivable failure could occur. In general only those systems or components which are judged to have a credible chance of failure are assumed to fail. Numerous failure modes are generally not evaluated within the accident analyses (i.e., partial failures, pump failures at some time during the event, etc). Nor are instrument and control systems or emergency procedures designed to cover all conceivable failure modes. The single failure criterion has been applied via static analyses as a system functional design criteria to assure each redundant system is capable of mitigating the consequences of an accident. The pre-EDSFI SITA audit included a finding which recommends that a single failure analysis of the electrical distribution system be performed for the worst case single failure, including those occurring after T=0.

This document establishes that the Oconee licensing basis only requires consideration of single failures "immediately on demand" for emergency power<sup>1</sup>; Section I below details licensing basis issues. Correspondence and numerous reports have been reviewed to identify the licensing basis for Oconee with regard to the timing of single failures. This review indicates that nothing within the Oconee licensing basis specifically requires consideration of single failures at times other than "immediately on demand" (vs T = 0, or coincident with the event).

Section II briefly reviews the safety significance of excluding consideration of single failures which occur at times other than immediately on demand.

## I. LICENSING BASIS

### I.A Discussion:

The earliest discussions of single failure appear during the construction permit application review. The electrical system design was obviously changed during the course of the review. In Reference 5, Duke describes the various power sources and the following "subsystems:" 230kV SY emergency switching, Keowee automatic startup and switching, emergency power source automatic switching, and engineered safeguards auxiliary load-shedding. The sources identified are significantly different than those licensed (i.e., the first alternate unit through the main feeder buses or through the 230kV SY and the 4160V auxiliary

---

<sup>1</sup> The licensing basis review focused on single failure issues related to emergency power. Expanding the scope to include all mechanical systems will require further review.

electrical system). Logic diagrams are provided, however time delays associated with transfers are not identified. The AEC staff reviewers concur with the design approach since it is an effective and simple way of implementing the single failure criterion (Ref 6).

The original FSAR and (then draft) IEEE-279 establish the single failure criterion as a requirement<sup>2</sup>. Each of these documents specify the single failure criterion differently, and no guidance regarding interpretation of the single failure criterion was provided during initial licensing:

- Original FSAR, Section 1A.39 "Criterion 39 - Emergency Power For Engineered Safety Features"

"Alternate power systems shall be provided and designed with adequate independency, redundancy, capacity, and testability to permit the functioning required of the engineered safety features. As a minimum, the on-site power system and the off-site power system shall each, independently, provide this capacity assuming a failure of a single active<sup>3</sup> component in each power system."

- IEEE 279-1971, Section 4.2

"Any single failure within the protection system shall not prevent proper protective action at the system level when required."

During the AEC staff review for the Oconee operating license, the staff was concerned that all three ES buses received power from only one emergency source at a time. The staff requested an analysis of the design to show that the independence and reliability of the redundant ESF loads are as good as that provided by a split bus design (Ref 7). Duker's response was provided by submitting FSAR Revision 7 (Ref 9). Prior to receiving FSAR Revision 7, the staff reported to the ACRS (Ref 8) that "at present we believe that the applicant will be able to show that the Oconee design is acceptable, based on the large number of power sources, the relatively large capacity of these sources, and the high reliability of the hydro units." Thus, it can be inferred that the staff

---

<sup>2</sup> Appendix K (ECCS Evaluation Models) was going through the rulemaking process during Oconee licensing. It was approved after all three Oconee Units received their operating licenses, however it is considered part of the licensing basis since it is the basis for acceptability of the B&W LOCA Topical Reports.

<sup>3</sup> The Oconee licensing basis does not provide a specific definition of passive and active single failures of electrical equipment. However, active failures have generally been interpreted to include such things as failure of an open breaker to close; passive failures include such things as a bus fault. 10 CFR 50, Appendix A, the General Design Criteria, is interpreted by the NRC staff in SECY 77-439 to require that there be no distinction between active and passive failures for electrical equipment. The GDCs are not part of the Oconee licensing basis. Therefore, for Oconee, a distinction can be made between active and passive failures.

did not expect consideration of smart single failures to be the basis for acceptability. Rather, it appears that the concept of defense in depth and reliability were dominant. Duke responded to the concern by submitting FSAR Revision 7 (Ref 9). Dukes' interpretation of Criterion 39 and IEEE 279-1971 resulted in the inclusion of the following sections:

- Original FSAR, Section 8.2.3.3

"The basic design criteria of the entire emergency power system of a nuclear unit, including the generating sources, distribution system and controls, is that a single failure of any component passive or active will not preclude the system from supplying emergency power when required." Note that this section does not respond to the two single failures required by Criterion 39.

- Original FSAR, Section 8.2.3.3C

"The redundant transfer logic will seek the most available source of power and when it becomes available close into it. If the source is then subsequently lost, the switching logic and equipment will transfer to the other source automatically." This statement is not considered to be the bounding design criterion for the electrical system, rather it merely identifies transfer logic response to the loss of a power source.

FSAR Revision 7 did not provide a detailed analysis of the various timers in the EPSL design, nor did it provide a detailed description of the methodology used to perform the single failure analyses. This FSAR Revision as well as previous and subsequent revisions did include several system single failure analyses. Review of these analyses shows that each single failure evaluated occurred immediately on demand<sup>4</sup>. No single failures were identified which occurred at any other time than immediately on demand. For example, single failures where a transformer loaded, then failed at some later time were not considered. These analyses were found acceptable by the AEC staff (simply based on the fact that the operating license was issued). The Oconee SER (Ref 11) describes the sources of power which are automatically connected to the main feeder buses, the order they are connected, and sources which can be made available manually. The SER does not describe EPSL, nor does it describe the basis for the acceptability of the design of the onsite power system (e.g., Criterion 39 is not mentioned, GDC 17 is not mentioned, single failure criteria is not mentioned). The SER simply concludes that the onsite power system is acceptable.

Subsequent to issuance of the operating licenses, the licensing basis was expanded to include the following:

- 10 CFR 50, Appendix K Section I.D, Post-Blowdown Phenomena, includes the

---

<sup>4</sup> This conclusion is simply based on the fact that had the analyses considered single failures occurring at any time other than immediately on demand, the results would have been unacceptable.

following criterion: "1. 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."

- FSAR Section 6.3.1 "... (ECCS) is designed to tolerate a single active failure (short term) or a single active or passive failure (long term)." The long term phase is generally assumed to begin when the ECCS is transferred to the sump recirc mode. This requirement expands the scope of single failures to include passive failures in the long term, however it is silent on the timing of the failure (e.g., on demand or otherwise).

The B&W LBLOCA Topical Reports (BAW-10103, and BAW-10104) and the SBLOCA Topical Report (BAW-10154) have been evaluated based on the criteria in Appendix K. The worst case single failures identified are those which produce the minimum ECCS injection<sup>5</sup>. For both the LBLOCA and SBLOCA topicals, worst case single failure is assumed to be loss of a diesel which results in the operation of only one LPI pump and one HPI pump. Specific consideration is not given to timing of the diesel failure. These topical reports have been reviewed and approved by the NRC. Specific analyses have been performed by B&W to show the acceptability of the additional time required to supply ECCS due to single failure of CT-4 (immediately on demand) with retransfer to startup (Ref 12).

In 1990, the single failure timing issue was raised internally. Reference 13 concluded that the initial design criteria for the ECCS did not consider a single failure occurring at some other time than initiation of the accident (e.g.,  $T = 0$ ), and there is no requirement to identify the worst time when the worst case single failure will occur. The pre-EDSFI SITA auditors took issue with the " $T = 0$ " position. This position has been further refined as a result of this research to include any single failure occurring immediately on demand, rather than those occurring spuriously at initiation of the accident.

Based on the above, the current licensing basis does not require consideration of single failures at times other than immediately on demand for emergency power. Within the Oconee licensing basis, the concepts of defense in depth and reliability establish the basis for acceptability rather than a specific interpretation of one design criterion.

---

<sup>5</sup> Other than a statement to the effect that the worst case single failures are those which produce minimum ECCS injection, the topicals do not provide the methodology used to determine the worst case single failure. Informal conversations with B&W engineers responsible for development of these topicals indicates that "once it starts it runs" is an unwritten assumption in the analyses.

I.B Relevant Guidance not within the Oconee Licensing Basis:

The following guidance documents are identified for information purposes only since they are not part of the Oconee licensing basis:

- IEEE379-1972/N41.2, "Standard for Application of the Single Failure Criterion to Nuclear Power Generating Station Class 1E Systems"

No commitments to this have been identified. This standard does not specify timing considerations for single failures.

- SECY 77-439, "Single Failure Criterion"

The staff states that a single failure evaluation "... proceeds on the proposition that single failures can occur at any time." The Oconee position is in direct contradiction to this portion of the guidance. However, the SECY paper concludes that "the single failure criterion has served well in its use as a licensing review tool to assure reliable systems as one element of the defense in depth approach to reactor safety."

- ANSI/ANS 58.9-1981 "Single Failure Criteria for LWR Safety-Related Fluid Systems"

During the short term, the single failure considered may be limited to an active failure. An active failure is defined as a malfunction excluding passive failures of a component that relies on mechanical movement to complete its intended function upon demand.

- Standard Review Plan Section 6.3.II (p6.3-4) 7/81

The ECCS should retain its capability to cool the core in the event of a failure of any single active component during the short term immediately following an accident, or a single active or passive failure during the long-term recirculation cooling phase following an accident.

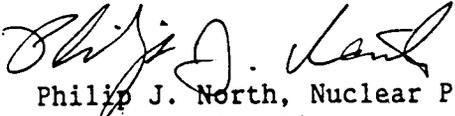
II. SAFETY SIGNIFICANCE

The Severe Accident Analysis Group analyzed the single failure timing issue to determine the credibility of worst case timing events. Reference 14 concludes that the most probable failures are those where the component is in an initially failed or unavailable state. In addition, the postulated single failures are either insignificant probabilistically, or are not the last defense in core damaging sequences.

### III. CONCLUSIONS

It is clear that there is no requirement within the Oconee licensing basis to analyze for "smart" single failures. It is also clear that analyses performed in support of Oconee licensing made no effort to include these single failures. The single failure criterion, as interpreted within the Oconee licensing basis, is one of many elements of the defense in depth approach to reactor safety. In the specific case of the Oconee electrical distribution system, the large number of power sources, the relatively large capacity of these sources, and the high reliability of the hydro units provide additional defense in depth. This position is compatible with work done in support of the Oconee PRA.

M. E. Patrick, Regulatory Compliance Manager  
Oconee Nuclear Station

  
By: Philip J. North, Nuclear Production Engineer  
Regulatory Compliance

xc: H. B. Barron, ONO1VP  
J. M. Davis, ONO1VP  
R. L. Sweigart, ONO101  
B. L. Peele, ONO1VP  
R. L. Dobson, ONO2EE  
B. J. Dolan, ONO2ME  
D. M. Jamil, ONO2EE  
D. B. Coyle, ONO1SE  
R. L. Gill, EC050  
K. S. Canady, EC08H  
G. B. Swindlehurst, EC08H  
P. M. Abraham, EC08I  
A. V. Carr, PB05E  
File

### REFERENCES:

1. FSAR Section 3.1.39
2. 10 CFR 50, Appendix K. Section I.D, Post-Blowdown Phenomena; Heat Removal by the ECCS, "1. 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."

Single Failure Timing Licensing Basis  
Page 7

3. SECY 77-439, August 17, 1977 Single Failure Criterion, page 5 "The General Design Criteria make it clear that for electrical, instrumentation, and control systems, application of the Single Failure Criterion to systems evaluation depends not only on the initiating event that invokes safety action of these systems, together with consequential failures, but also on active or passive electrical failures which can occur independent of the event. Thus, evaluation proceeds on the proposition that single failures can occur at any time"
4. R. L. Gill to B. L. Peele, March 20, 1990. "All design basis accidents assume that the worst case single failure occurs at T=0.... A final conclusion that can be reached is that we are not required to identify the worst time when the worst case single failure will occur."
5. PSAR Supplement 2, Question 4.1, May 25, 1967
6. AEC Staff Report 2 to the ACRS (Construction Permit), June 16, 1967
- 7. Al Schwencer (AEC) June 16, 1970 telecon with Paul Barton (Duke), June 23, 1970 ✓
- 8. AEC Staff Report 1 to the ACRS (Operating License), page 49 July 24, 1970 ✓
- 9. FSAR Supplement 6 (includes FSAR Rev 7), August 11, 1970.
10. FSAR Section 6.3.1. "... (ECCS) is designed to tolerate a single active failure (short term) or a single active or passive failure (long term)."
11. Oconee Unit 1 SER Section 8.4, December 29, 1970
12. Oconee FSAR Section 15.
13. R. L. Gill to B. L. Peele, March 20, 1990
14. G. L. Cruzan to P. J. North, December 16, 1992

FOR LEN WIENS

~~FOR BILL RAUGHTLEY~~

January 29, 1993

MEMO TO FILE

Subject: Single Failure Design Criteria  
Summary of January 27, 1993 Meeting

Attendees: Duke  
Bob Dobson  
Dhiana Jamil  
Mark Patrick  
Steve Nader  
Paul Colaianni  
Phil North

NRC - EDSFI Team

Milt Shymlock

Walt Rogers

Keith Poertner

Bill Raughtley

On January 27, 1993 an informal meeting was held with the NRC EDSFI team to discuss the Oconee licensing basis with respect to single failure criteria. Interpretations of licensing basis criteria discussed at the meeting are described below:

#### Electrical Power System:

FSAR Section 3.1 lists draft AEC Criterion 39, "Emergency Power for Engineered Safety Features." Briefly, Criterion 39 describes the capability to withstand a single active failure in the onsite power system and an additional single active failure in the offsite power system. In response to this criterion, the FSAR states that "the intent" of the criterion is met as described in Chapter 8 of the FSAR. Chapter 8 of the FSAR describes a design criterion which differs from Criterion 39: "the basic design criterion of the entire emergency power system, . . . , is that a single failure of any component passive or active will not preclude the system from supplying emergency power when required;" (e.g., no "double failure" is identified in the Chapter 8 criterion). In the original SER, the NRC did not take exception to this method of meeting "the intent" of Criterion 39. The SER simply concludes that the onsite and offsite power systems are acceptable, without citing design criteria as the basis for acceptability. Therefore, the interpretation of Criterion 39, as described in Chapter 8 of the FSAR is the licensing basis for single failures in the emergency power system.

Regardless, it is believed that Oconee has the ability to meet the letter of Criterion 39, since only active failures must be postulated. Active failures of electrical components are those failures involving physical movement of a device when required, such as a breaker failing to trip or to close. Passive failures of electrical components are generally considered to include concerns such as faults.

## Single Failure Design Criteria Meeting

Page 2

Mechanical Systems:

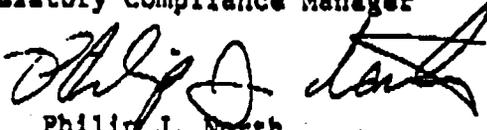
For mechanical systems, the single failure is either:

- 1) An active failure occurring during the short term, or
- 2) An active failure in any safety related system, or a passive failure in an ECCS system (HPI, LPI, Core Flood) occurring during the long term.

Equipment moving spuriously from the proper safeguards position is generally excluded from consideration as a single failure. However, a single failure of a manually controlled, electrically-operated valve in an ECCS system is considered.

It is expected that these issues will be further clarified in the Oconee Single Failure Criterion Design Basis Document. This DBD is planned to be issued in 1993.

M. E. Patrick  
Regulatory Compliance Manager

  
By: Philip J. North  
Nuclear Production Engineer

xc: Attendees  
R. C. Gamberg  
A. V. Carr  
B. J. Dolan  
R. L. Sweigart  
D. V. Deatherage  
B. L. Paele  
D. B. Coyle  
File

LEN,

THE LICENSEE STATED THAT THEIR VIEW OF "SINGLE FAILURE" AS IT RELATES TO OPERATOR ERROR WAS ONLY APPLICABLE TO THE OCONEE CONTROL ROOM NOT KEOWEE. ALSO, THE OPERATOR ERROR WAS THE MIS-POSITIONING OF A VALVE THAT COULD BE OPERATED FROM THE CONTROL BOARD. OPERATOR ERROR DID NOT EXTEND INTO THE PLANT.

THE LICENSEE INDICATED THAT PAST NRR DISCUSSIONS ON PASSIVE SINGLE FAILURE FROM A MECHANICAL STANDPOINT WAS INTERPRETED BY OCONEE TO BE APPLICABLE TO ECCS - HPI, LPI NOT ECCS SUPPORT SYSTEMS SUCH AS KEOWEE.

Thanks,

Walt Rogers



# Oconee Nuclear Station

## Problem Investigation Process

### Problem Investigation Form

<b>PIP Serial No:</b> 4-095-1686	<b>LER Serial No:</b>
<b>MSE Serial No:</b>	<b>Other Report:</b>

to verify the Keowee units will start and carry the emergency loads for a specified time was not observed.

The Keowee test procedures reviewed did not specify a minimum unit run time to allow a correlation between the design basis run time of seven days and support system requirements nor was there documented justification for not performing the testing. Several other design basis calculations have not been proven by the test procedures to date. For example:

- Turbine Guide Bearing Oil Reservoir level control greater than 4.5 inches
- Turbine Guide Bearing Oil temperature control at 167 degrees
- Air Circuit Breaker supply air reservoir minimum pressure
- Lower Oil Reservoir temperature control greater than 80 degrees
- Governor Oil Pressure Tank level and pressure at 62.47 inches and 350 psig
- Governor Oil sump temperature below 130 degrees
- Governor Oil Pressure Tank pressure and level
- Generator Air and Thrust Bearing temperature control
- Turbine Sump level control

2. An observation of the Testing Keowee Overhead ACBs TT/0/A/0610/11, was conducted. The purpose of testing was to gather information and data on the operation of the Keowee Air Circuit Breakers (ACB) when air supply is not available. Facts noted and observation included the following:

- The Design Basis of 145 psig minimum air reservoir pressure was not conclusively verified by the test method.
- An Oconee Control Room SRO was not notified by the test procedure steps.
- The approved test procedure results are documented by a calculation (OSC-5556). The calculation references and attaches a plant file memorandum, Addendum-4, Attachment-5.

In addition to the above concerns, the following memorandum statement highlights the test results versus the Design Basis:

"The 118# pressure switch, which had been set to trip the ACBs and clear the overhead power path, actuated during both the ACB1 and ACB2 140# tests, as evidenced by a computer point actuation. The pressure switch did not actuate during the 150# tests. Worst case past operability with the trip installed, assuming loss of the air supply system, and assuming 140# of air in the cylinder, the overhead ACB would not have closed due to the trip signal. With 150#, no air supply, and assuming 5#/hr leakage, the overhead path would have tripped within a couple of hours."

- a. As a result of the calculation, administrative controls or contingency plans are not in place to assure makeup air is available based on reservoir leakage or based on air compressor availability.
- b. The Design Basis of 145# air reservoir pressure baseline is questionable.
- c. Critical test results are documented in the memorandum. The calculation and results (memorandum) should be incorporated into an approved test procedure.

# Oconee Nuclear Station

## Problem Investigation Process

### Problem Investigation Form

<b>PIP Serial No:</b>	4-O95-1686	<b>LER Serial No:</b>	
<b>MSE Serial No:</b>		<b>Other Report:</b>	

d. Acceptance Criteria of test is "None". Acceptance criteria would be appropriate based on the Design Basis.

3. There is not a documented plan for testing the integrity of the underground feeder cables.

Originated By: JASTANDR Team: JMF8306 Group: QVD Date: 12/15/95

Last Updated By: JASTANDR Team: JMF8306 Group: QVD Date: 12/15/95

Last Updated By: JASTANDR Team: JMF8306 Group: QVD Date: 12/15/95

Last Updated By: JASTANDR Team: JMF8306 Group: QVD Date: 12/15/95

Last Updated By: JASTANDR Team: JMF8306 Group: QVD Date: 12/15/95

Other Units/Components/Systems/Areas Affected (Y,N,U): N

Industry Plants Affected (Y,N,U): U

Immediate Corrective Actions:

Problem Found While Working with Document No. :

Immediate Corrective Action Work Request / Work Order No. :

	<u>Indiv</u>	<u>Team</u>	<u>Group</u>	<u>Date:</u>
Problem Identified By:	JASTANDR	JMF8306	QVD	12/15/95
Problem Entered By:	JASTANDR	JMF8306	QVD	12/15/95

**II. Significance**

Is the Problem Significant? N Action Category: 3

OEP No:

Other Report Nos:

Event Codes: F8 Testing

# Oconee Nuclear Station Problem Investigation Process Problem Investigation Form

<b>PIP Serial No:</b> 4-O95-1686	<b>LER Serial No:</b>
<b>MSE Serial No:</b>	<b>Other Report:</b>

O6

SITA

**Screening Remarks:**

This event does not meet the MSE significance criteria, screened by the CST.

Originated By: HDUMEYER Team: LVW7310 Group: SRG Date: 12/18/95

Responsible Group for Proposed Resolution(s):	SES	Systems Engineering
Responsible Group for Problem Evaluation:	SES	Systems Engineering
Responsible Group for Overall PIP approval:	QVD	Regulatory Audits

Screened By:	<u>Indiv</u>	<u>Team</u>	<u>Group</u>	<u>Date:</u>
	HDUMEYER	LVW7310	SRG	12/18/95

### III. Problem Evaluation

System(s) Affected:	J	Jocassee
	K	Keowee

Affected Equipment:	Comp.	Manufacturer
<u>WMS Equipment ID No.</u>	<u>Code</u>	<u>Name</u>

<b>Problem Evaluation:</b>	<b>Group:</b>	SES	<b>Status:</b>	ReadyForQVD
----------------------------	---------------	-----	----------------	-------------

**Response to Observation #1**

Oconee documented its position on the adequacy of testing on the Keowee emergency power system and components in a November 17, 1995 submittal to NRC. Specifically, Oconee's response to NRC question #1 addresses observation #1 of this PIP. Following are excerpts from that submittal.

Testing of the emergency power systems is performed with great thoroughness. During the development of the testing, all design basis criteria were considered. Integral testing on the system level is performed when practical and the functions and logic are verified to the component level. The testing and supporting analysis of the emergency power system comply with or exceed the requirements of the Technical Specifications. The Oconee emergency power system meets its design basis and the testing demonstrates the capability of the system to perform its intended design functions.

Both periodic and one-time tests have been or are being performed to demonstrate the ability of the emergency power sources to perform their required design basis functions. These tests include the following:

**PERIODIC/ONE-TIME**

1. PT/0/A/0620/16 - Keowee Emergency Start Test

# Oconee Nuclear Station

## Problem Investigation Process

### Problem Investigation Form

<b>PIP Serial No:</b> 4-O95-1686	<b>LER Serial No:</b>
<b>MSE Serial No:</b>	<b>Other Report:</b>

2. PT/0/A/0610/22 - Degraded Grid and Switchyard Isolation Functional Test
3. PT/1,2,3/A/0610/01J - Emergency Power Switching Logic Functional Test
4. Keowee Load Rejection Test (Post NSM ON-52966 implementation)
5. TT/0/A/0650/01 - Keowee Black Start Test
6. Keowee Overhead Path & RCP Motor Load Test
7. PT/0/A/0610/19 - 100kV Power Supply Prior To Extended Keowee Outages
8. PT/0/A/0610/06 - 100kV Power Supply From Lee Steam Station
9. PT/0/A/0610/23 - Lee Gas Turbine Operation To the Grid Verification
10. Lee Combustion Turbine & ASW Motor Test
11. Keowee Low Power Test (scheduled for 11/22/95)
12. PT/1,2,3/A/0610/01A - EPSL Normal Source Voltage Sensing Circuit
13. PT/1,2,3/A/0610/01B - EPSL Startup Source Voltage Sensing Circuit
14. PT/1,2,3/A/0610/01C - EPSL Standby Bus Voltage Sensing Circuit

The Keowee Emergency Start Test (Test 1) is a periodic test that demonstrates Keowee's ability to emergency start upon receipt of a Keowee emergency start signal. In addition, it verifies the ability of the Keowee units to accelerate to rated speed and voltage within the committed time of 23 seconds. Achieving rated speed and voltage within 23 seconds allows ECCS injection to occur within the time assumed in the large break LOCA analyses. Also, this test demonstrates Keowee's ability to supply the equivalent loads of an Oconee LOCA/LOOP unit and two Oconee LOOP units. In accordance with the Technical Specifications, the capacity of the Keowee units is verified by accepting load from the system grid at the maximum practical rate. Keowee routinely demonstrates its capability to supply power in excess of the emergency loads when it generates to the system grid. The loading of a Keowee unit which is isolated from the system grid is performed in other periodic tests discussed below. In addition, the overhead generator breaker re-closing timer setpoints are verified during this periodic surveillance.

The Degraded Grid and Switchyard Isolation Functional Test (Test 2) periodically demonstrates Keowee's ability to separate from the system grid (load reject) upon receipt of a Keowee emergency start signal. During the test, Keowee energizes the overhead path up to the startup breakers for each Oconee unit following completion of the 230 kV switchyard isolation. When a LOOP or degraded grid concurrent with an ES signal occurs, the 230 kV switchyard Yellow Bus isolates from the system grid and aligns to the overhead path. This test ensures that either channel of the dual channel switchyard isolation logic can isolate the Yellow Bus from the system grid and align each Oconee unit startup transformer to the overhead path. During the test, the Keowee units receive an emergency start as a result of the simulation of a degraded grid concurrent with an ES actuation. The overhead unit, which is connected to the grid, load rejects by tripping its overhead generator breaker and automatically realigns itself to energize the overhead path. Also, the underground Keowee unit starts upon receipt of the emergency start signal and runs in standby. The acceptance criteria of this test include verification of proper breaker alignments in the switchyard, load rejection of the overhead Keowee unit, and verification of the alignment of the overhead power path. Since Oconee generation is not prohibited by the switchyard isolation, this test is performed with the Oconee units on line. Therefore, no Oconee auxiliary loads are available to be loaded onto the overhead Keowee unit. The capability of the overhead path equipment to carry loads equivalent to the emergency needs of the Oconee units is routinely demonstrated during shutdown, startup, and following reactor trip of an Oconee unit. The Degraded Grid and External Grid Protection System voltage relay setpoints and operation are verified in their specific relay maintenance/calibration procedure.

The Emergency Power Switching Logic Functional Test (Test 3) is a periodic test that demonstrates primarily the capability of the emergency power switching logic (EPSL) to adequately transfer the Oconee auxiliary loads to an

# Oconee Nuclear Station

## Problem Investigation Process

### Problem Investigation Form

PIP Serial No: 4-095-1686

LER Serial No:

MSE Serial No:

Other Report:

available power source. This test is performed during the refueling outage on each Oconee unit. The Keowee underground unit, Lee combustion turbine (CT) and offsite power are used as sources of power during this switching logic test. Transfer of the Main Feeder Busses (MFBs) from the normal source to the startup source, startup source to the standby bus and re-transfer back to the startup source are demonstrated during this test. Since the non-essential loads are shed prior to transferring to the standby bus, both channels of the load shed logic are verified to actuate during this test. Upon loss of the startup source, the undervoltage logic for the reactor coolant pump motors is verified to trip. During the test, actual auxiliary loads of the shutdown Oconee unit are transferred to the different sources. Keowee's ability to emergency start as a result of a simulated LOOP and LOCA is demonstrated during this test. For the Unit 1 EPSL test, the Keowee underground unit black starts since its auxiliary loads are lost as a result of a simulated LOOP on Oconee Unit 1.

This test was configured differently prior to 1987. Upon loss of the startup source (simulated LOOP), the auxiliary loads were transferred to the standby busses and loaded onto an accelerating Keowee underground unit. Since 1987, the transfer to the standby busses occurs with the standby bus energized by a Lee combustion turbine. The simulated loss of the Lee CT then results in an automatic dead bus block transfer of loads to an idling Keowee unit. This evolution verifies the EPSL logic between the SL and SK breakers. During these transfers, a Lee CT supplies power to the Oconee auxiliary loads for approximately 60 minutes and Keowee provides power to the Oconee loads for one to two hours. Instability of a Keowee unit or Lee CT would be identified by either the Oconee, Keowee or Lee control room operators. This test is performed two to three times a year and no stability concerns have been identified. In order to document the stability of the Keowee units, voltage and frequency monitoring of the Keowee unit supplying Oconee will be performed periodically beginning with the present Oconee Unit 1 outage.

As a prerequisite to this EPSL test, the undervoltage logic for the normal, startup and standby sources is performed to ensure the 2 out-of-3 logic is functioning properly by Tests 12, 13 and 14, respectively. Each relay in the undervoltage logic and the associated auxiliary relays are verified to ensure that the logic functions properly. The transfer time delay relay setpoints and undervoltage relay setpoints for both the 4 kV and 7 kV systems are verified in their own respective calibration procedure.

Following the implementation of modification ON-52966, a Keowee Load Rejection Test (Test 4) will be performed periodically. This modification adds overfrequency protection, governor failure monitoring and governor failure protection to the Keowee units. This test verifies the ability of the Keowee units to load reject and return to normal speed within the required time. Appropriate instruments, such as the MW/VAR meter and frequency relays, are calibrated by their respective procedures prior to this surveillance test. Tripping of the Keowee generator breaker on emergency start and re-closing within the appropriate timeframe is demonstrated during this transient. Successful realignment to the appropriate power path within the defined time is the acceptance criterion for this test.

As part of the design of this modification, several Keowee load rejection tests were performed to collect data associated with the response of the Keowee units to a loss of load. These tests were performed at power levels ranging from 60 to 90 MW and consisted of both single and dual unit load rejections. Actual emergency start signals were used to initiate each load rejection.

A Keowee Black Start Test (Test 5) demonstrated Keowee's ability to emergency start with only DC power (black start) available to its auxiliaries. The black start feature was part of the original Keowee design and was tested as part of the pre-operational startup testing for Keowee. This feature was reverified during a one-time test in December of 1992. As mentioned in the description of Test 3, whichever Keowee unit is connected to the underground path is black started during each Oconee Unit 1 EPSL functional test. Although the black start test is

# Oconee Nuclear Station

## Problem Investigation Process

### Problem Investigation Form

**PIP Serial No:** 4-O95-1686

**LER Serial No:**

**MSE Serial No:**

**Other Report:**

considered a one-time test, this feature is demonstrated on a routine basis. As at Oconee, the DC system at Keowee is monitored and tested periodically. Along with other periodic battery preventative maintenance, service and performance tests are conducted to demonstrate that the DC system is performing as designed.

A one-time test of the Keowee Overhead Path with a Reactor Coolant Pump (RCP) Motor Load (Test 6) was performed on May 31, 1993 to collect data for the certification of a computer model. During the test, a 9000 hp RCP motor was block loaded onto an idling Keowee overhead path unit. The block loaded RCP motor resulted in an inrush MVA that was larger than the LOCA loads of an ONS unit. Since the purpose of this test was to obtain data, no test acceptance criteria were established. The Keowee unit accepted this load as expected. Calculation OSC-5336 documents the correlation between the test data and the computer model simulation.

The Keowee Low Power Test (Test 11) is scheduled to be performed during the present Oconee Unit 1 refueling outage as part of the EPSL test. The Keowee underground unit is loaded as it accelerates to rated speed and voltage which is similar to the EPSL test prior to 1987. When the Keowee unit is at steady-state, blocks of load are added and rejected from the Keowee unit. This test will collect data on the Keowee unit during the load transients.

Descriptions of Tests 7 through 10 can be found in the submittal to NRC. They have been omitted from this proposed resolution because they deal with Lee combustion turbines and the 100kV path.

Keowee and Lee generate to the system grid for commercial peaking power. A majority of the circuits and functions that must operate for grid generation are the same circuits and functions that operate during an emergency. Grid generation reduces the amount of time that failures are left undetected in certain circuits. The ability to use these sources for commercial power generation is an asset to the emergency power system.

Oconee bridges the gap between testing and actual design requirements by using analysis. Since actual design basis loads are not available for functional testing, computer models are used to ensure the full loading capability of the emergency power sources. The computer modeling tool which is used at Oconee is the CYME program. The CYME program is capable of dynamically modeling the power source and the electrical loads. Certification testing and analysis for the CYME program have been performed for Keowee and Lee. The voltage adequacy analysis for the Oconee auxiliaries has been performed for the Keowee overhead path, Keowee underground path, and Lee CTs. This analysis includes the worst case design accident loads. In addition, failures are postulated which result in the loading of additional non-essential loads. The possibility of the generator terminal voltage operating below nominal has been considered by the analysis. Finally, the addition of loads for the non-accident units after the accident loads of the affected unit has been analyzed to cover the possible transfer scenarios. Other combinations of possible loadings between ONS units have been analyzed.

Observation #1 of this PIP also listed some examples of support systems which the SITA team believed were not adequately tested. The SITA recommended tests for such things as sump level control, Governor Oil sump temperature below 130 F, and such. Most of these items are calibrated and monitored by alarms at all times. Some, such as the Governor Oil Sump temperature, were deemed to be remote enough in occurrence, that the manufacturer makes no provision for monitoring this temperature other than feeling the sump. Since these items are monitored all the time, and are in the worst case condition during system generation, there is no need for a test which shows the same thing as normal operation.

Response to Observation #2

# Oconee Nuclear Station

## Problem Investigation Process

### Problem Investigation Form

<b>PIP Serial No:</b>	4-O95-1686	<b>LER Serial No:</b>	
<b>MSE Serial No:</b>		<b>Other Report:</b>	

- see proposed resolution -

Response to Observation #3

- see proposed resolution

Originated By: LJAZZARE Team: DBC7309 Group: SES Date: 01/15/96

Last Updated By: LJAZZARE Team: DBC7309 Group: SES Date: 01/15/96

Event	Cause Cd	Cause Description	Primary	Causing Group(s)
F8	B3	Method of Presentation	No	ESE
F8	N/A	Not Applicable	Yes	SES

Responsible Group(s) for Proposed Resolution: SES Systems Engineering

	Indiv	Team	Group	Date
Accepted By:	SWBALDWI	LJA2713	SES	12/18/95
Assigned To:	LJAZZARE	LJA2713	SES	12/18/95
Due Date:	01/27/96			
Ready for Approval:	LJAZZARE	DBC7309	SES	01/15/96
Approved By:	SWBALDWI	LJA2713	SES	01/16/96

Proposed Resolution From: Response to Observation #1: Group: SES Status: ReadyForQVD

No further actions are needed in response to this observation. Justification is provided in the cause evaluation which demonstrates that current testing is adequate to demonstrate Keowee emergency power design basis and 10CFR50 Appendix B Criterion XI, Test Control.

Response to Observation #2

The purpose of TT/0/A/0610/11 was to gather data on the operation of Keowee ACBs. It was not written or intended to conclusively verify 145 psig as the design basis for minimum air reservoir pressure. The test method was adequate for its intended purpose. In addition, it is common to not include test criteria for tests which are intended to just gather data. Acceptance criteria is, and will continue to be, included for tests that verify design basis. No further corrective actions are needed.

Until NSM-52966 is fully implemented, Operations rounds sheets contain direction to check ACB air pressure. NSM-52966 will raise the normal operating pressure of the ACBs from 150 psig to 160 psig. It will also raise the low air pressure alarm for the ACB from 118 psig to 150 psig. The NSM also adding two new pressure switches to the headers which will also alarm at 150 psig. All this ensures that adequate air pressure will exist for the ACB to perform its intended design function. No further corrective actions are needed.

# Oconee Nuclear Station Problem Investigation Process Problem Investigation Form

<b>PIP Serial No:</b>	<b>4-095-1686</b>	<b>LER Serial No:</b>
<b>MSE Serial No:</b>		<b>Other Report:</b>

An internal memorandum is referenced by calculation OSC-5556. This memo contains results obtained during the performance of TT/0/A/0610/11. The calculation should actually reference the test procedure directly, with all relevant information contained in either the test procedure or the calculation. OSC-5556 will be revised to directly reference the test procedure and not leave relevant information solely in the memorandum.

It is true that TT/0/A/0610/11 did not contain a step which directed the test coordinator to notify the Control Room SRO before initiating certain test procedure steps. However, the Keowee overhead ACB being tested was taken out-of-service per Operations procedure. The expectation of Operations management is that the Control Room SRO be aware/notified of equipment that is removed from service. Taking the equipment out-of-service per Ops procedure is considered to be adequate notification that the equipment is not available. It is NOT the expectation of Operations management that the Control Room SRO be notified at various steps/points in the test procedure, given that they are aware that the equipment is out-of-service. The testing did not impact the ability of one Keowee unit to feed the overhead path and the other Keowee unit to feed the underground path (no LCO was entered). Therefore, the test procedure is not considered inadequate. No further corrective actions are needed in response to this concern.

### Response to Observation #3

Testing of the integrity of the underground feeder cables has previously been identified as an issue and is being tracked by PIP 95-0611. Engineering (ESE) has created a project and placed it in PLAN (ON-95-0683) which details the specific activities associated with this project. PIP 95-0611 and PLAN project ON-95-0683 reference each other. PIP 95-0611 will track this issue. No further corrective actions are needed.

Originated By: LJAZZARE Team: DBC7309 Group: SES Date: 01/08/96

Last Updated By: LJAZZARE Team: DBC7309 Group: SES Date: 01/08/96

Last Updated By: LJAZZARE Team: DBC7309 Group: SES Date: 01/08/96

Last Updated By: LJAZZARE Team: DBC7309 Group: SES Date: 01/15/96

Last Updated By: LJAZZARE Team: DBC7309 Group: SES Date: 01/15/96

Last Updated By: LJAZZARE Team: DBC7309 Group: SES Date: 01/15/96

# Oconee Nuclear Station Problem Investigation Process Problem Investigation Form

PIP Serial No:	4-095-1686	LER Serial No:	
MSE Serial No:		Other Report:	

Last Updated By: LIAZZARE Team: DBC7309 Group: SES Date: 01/16/96

Accepted By:	Indiv	Team	Group	Date
Assigned To:	SWBALDWI	LJA2713	SES	12/18/95
Due Date:	LIAZZARE	LJA2713	SES	12/18/95
Ready for Approval:	01/27/96			
Approved By:	LIAZZARE	DBC7309	SES	01/16/96
	GKMCANIN	DBC7309	SES	01/16/96

Remarks:

Corrective Actions

Seq. No:	1
----------	---

Resp Group: ESE  
 Orig Group: SES  
 Event Code: F8  
 Cause Code: B3

Comments  
 Revise calculation OSC-5556 to directly reference test procedure TT/O/A/0610/11, instead of referencing the internal memorandum (PROFS note). Ensure all relevant information resides in either the calculation or the test procedure (the memo should not be the sole residence of any important information).

Originated By: LIAZZARE Team: DBC7309 Group: SES Date: 01/15/96

Proposed Corrective Action

Outage:  
Tracking

Assigned To:  
Ready for Approval:  
Approved By:

Indiv  
LIAZZARE  
SWBALDWI  
SWBALDWI

Mode:

Prop CAC: Closed

Team	Group	Date
LJA2713	SES	01/16/96
LJA2713	SES	01/16/96
LJA2713	SES	01/16/96

Actual CAC: ReadyForQVD  
Due Date: 03/14/96

Actual Corrective Action Resolution From:

Comments  
 Calculation OSC-5556 was revised (per Rev. 2) to include reference to test procedure TT/O/A/0610/11 associated with Keowee ACB air testing. No further action is necessary for this CA.

Originated By: HTGRANT Team: TAL8382 Group: ESE Date: 03/11/96

Accepted By:  
Assigned To:  
Due Date:  
Ready for Approval:

Indiv  
BEMCALIS  
HTGRANT  
03/14/96  
HTGRANT

Team	Group	Date
CAL7344	ESE	01/17/96
TAL8382	ESE	01/17/96
TAL8382	ESE	03/11/96

# Oconee Nuclear Station Problem Investigation Process Problem Investigation Form

PIP Serial No:	4-095-1686	LER Serial No:
MSE Serial No:		Other Report:

Approved By: TALEDFOR CAL7344 ESE 03/11/96

## V. Final and Overall PIP Approval

Criterion XVI Review:  
XVI Review Not Required for this PIP.

<u>Overall PIP Approval:</u>	<u>Indiv</u>	<u>Team</u>	<u>Group</u>	<u>Date</u>
Accepted By:	DWJENNIN	JMF8306	QVD	12/19/95
Assigned To:	JASTANDR	JMF8306	QVD	12/19/95
Due Date:	02/18/96			
Ready for Approval:				
Approved By:				

Closure Document Type

Closure Document No

Supplemental Concurrences - These do not affect PIP closure.

Concurrences Associated with External Commitments:

<u>Concurred By:</u>	<u>Indiv</u>	<u>Team</u>	<u>Group</u>	<u>Date</u>

## VI. Attachments

Environmental:  
No Environmental for this PIP.

Maintenance Rule:  
No Maintenance Rule for this PIP.

Failure Prevention Investigation:  
No FPI for this PIP.

# Oconee Nuclear Station

## Problem Investigation Process

### Problem Investigation Form

<b>PIP Serial No:</b> 4-O95-1686	<b>LER Serial No:</b>
<b>MSE Serial No:</b>	<b>Other Report:</b>

---

End of the Document for PIP No:4-O95-1686

The status of this PIP is: Screened  
The duration of this PIP was 3 days.

September 9, 1988

CTH  
only passes  
20 MW.

Memo To File

Subject: Keowee Hydro Station Operating Data  
File No. OS-203

The attached sheets contain a summary of Keowee's operating history by unit and year for the period covering January 1, 1980 through December 31, 1987. The information recorded on these sheets include the total number of unit demands and unit run hours per year, the number of unit demand and run failures, and the number of hours per year that each unit spent in "lockout maintenance" (i.e., not available for emergency use by Oconee). Also included on the data sheets are single and combined unit unavailabilities due to "lockout maintenance."

Several record sources were accessed for the above data. The number of unit starts and run hours were obtained by reviewing microfilm copies of daily Keowee Switchboard Logs. The data was recorded in a notebook which may be used for future reference. The unit demand and run failure data and the amount of "lockout maintenance" was obtained through an indepth review of Keowee's Operator Log books kept on site at Keowee.

The accuracy and timely manner in which this data was acquired is a direct result of the help and cooperation given to me by Keowee Hydro Station personnel.

If there are any questions, please contact Mike Miscabeimer (3-8833) or Don Azzarello (3-5006).

*C. M. Misenheimer*

By: C. M. Misenheimer  
Technical Associate

CMM/mew

cc: K. S. Canady  
P. M. Abraham  
B. J. Dolan  
R. L. Sweigart  
D. V. Deatherage  
L. J. Azzarello  
G. L. Cruzan  
Don Couch - Keowee

Unit will go  
up to 90 MW

Keowee Unit Failures (1980-1987)

	<u>Date</u>	<u>Unit</u>	<u>Start</u>	<u>Run</u>	<u>Description</u>
not valid	5-21-80	2	X	What is capacity of CT-4?	Oconee started unit for Dispatcher but couldn't get partial shutdown relay to pick up. Would only generate $\frac{2}{3}$ 90 MW max. Problem was loose wires on terminal board.
not valid	8-1-80	2	X		Voltage Regulator failed, unit started on second attempt.
valid failure	8-9-80	2	X ✓		Voltage Regulator failed. Relay K-5 had dirty contacts.
valid failure	9-25-80	2	X ✓		Governor would not bring turbine up to speed. Unit lockout.
	2-02-81	1		X	Fish in cooling water strainer. <i>Common Cause Failure to Run</i>
not valid	6-11-81	X 1	X		Unit would not come up to full load. (Wouldn't go above 64 MW)
valid	9-3-81	2	X	Not touched during maintenance	Generator UV relay operability and checkout. Unit started for operation check and tripped.
valid failure	6-22-82	1	X ✓		Unit started for operability check. Would not come up to speed. Governor pressure tank problem.
not valid	1-05-83	1	X		Unit failed to <sup>auto</sup> start due to relay malfunction. (Started locally) <i>This relay would not have affected emergency start. (Superior statement recorded in R.D. Log.)</i>
valid	6-16-83	1	X	Not touched during maintenance	Generator field flashing breaker relay 86EX-1 contacts did not make. Unit in maintenance (coming out)
Valid	8-10-83	1	X	Not touched during maintenance	Pressure switch, 1PS2 failed. (Unit coming out of maintenance)

Keowee Unit Failures (1980-1987)

	<u>Date</u>	<u>Unit</u>	<u>Start</u>	<u>Run</u>	<u>Description</u>
at valid	1-20-84	2		X	Ocong shutdown unit due to generator excitation alarm.
Valid	11-20-84	2	✓ X		Would not have interfered with emerg. operation. Would not have been shutdown Generator excitation supply breaker failure.
Valid	12-04-84	2	✓ X		Generator excitation supply breaker failure.
ne valid failure	7-5-85	1	✓ X	X	Governor will not bring turbine up to speed.
	7-8-85				
	7-9-85				
					Governor will not bring turbine up to speed. Governor repaired.
at valid	10-3-85	2		X	Unit would not parallel - regulator had dirty contacts. <i>Underground not lost</i>
Valid	11-19-85	2		X	Unit lockout due to generator field ground.
Valid	4-24-86	2		X	Generator excitation supply breaker will not close. Plunger sticks.
Valid	5-28-86	1		X	Generator field breaker will not close. Problem disappeared. <i>Unit started manually 6 minutes later</i>
at valid	7-2-86	1		X	Unit would not parallel to system. Speed adjust clutch problem. <i>Does it have to parallel to CTH?</i> <i>Bypassed in emergency</i> <i>Underground would be available</i>

In maintenance the whole time

*Underground not lost*

*Unit started manually 6 minutes later*

*Bypassed in emergency*  
*Underground would be available*

KEOWEE UNIT 1

	1980	1981	1982	1983	1984	1985	1986	1987	TOTAL
Number of Demands	327	341	269	345	349	288	327	331	2577
Number of Runhours	716.6	475.8	351.8	560.6	612.1	411.8	383.8	459.6	3972.1
Number of Demand Failures	0	0	1	3	0	3	2	0	9
Number of Run Failures	0	1	0	0	0	0	0	0	1
Hrs Of Lockout Maintenance (unit 1 only)	127.3	154.1	151.7	122.6	114.1	117.6	112.6	422.5	1322.5
Unavailability Due To Lockout (unit 1 only)	1.45%	1.76%	1.73%	1.40%	1.30%	1.34%	1.29%	4.82%	1.89%
Hrs Of Lockout Maintenance (both units)	1.5	37.1	29.4	1042.1	73.8	109.4	0	62.4	1355.7
Unavailability Due To Lockout (both units)	0.02%	0.42%	0.34%	11.90%	0.84%	1.25%	0.00%	0.71%	1.93%

Note: Yearly Unavailability = Yearly Lockout Hrs / Hrs in Year  
 Total Unavailability = Total Lockout Hrs / Total Years

KEOWEE UNIT 2

	1980	1981	1982	1983	1984	1985	1986	1987	TOTAL
Number of Demands	274	272	250	338	348	248	257	300	2287
Number of Runhours	585.2	282.4	244	539.4	513.9	311.9	281.9	429.1	3187.8
Number of Demand Failures	4	2	0	0	2	1	1	0	10
Number of Run Failures	0	0	0	0	1	1	0	0	2
Hrs Of Lockout Maintenance (unit 2 only)	119.9	153.4	136.4	109.8	444.1	93	122.7	67	1246.3
Unavailability Due To Lockout (unit 2 only)	1.37%	1.75%	1.56%	1.25%	5.07%	1.06%	1.40%	0.76%	1.78%
Hrs Of Lockout Maintenance (both units)	1.5	37.1	29.4	1042.1	73.8	109.4	0	62.4	1355.7
Unavailability Due To Lockout (both units)	0.02%	0.42%	0.34%	11.90%	0.84%	1.25%	0.00%	0.71%	1.93%

Note: Yearly Unavailability = Yearly Lockout Hrs / Hrs in Year  
 Total Unavailability = Total Lockout Hrs / Total Years

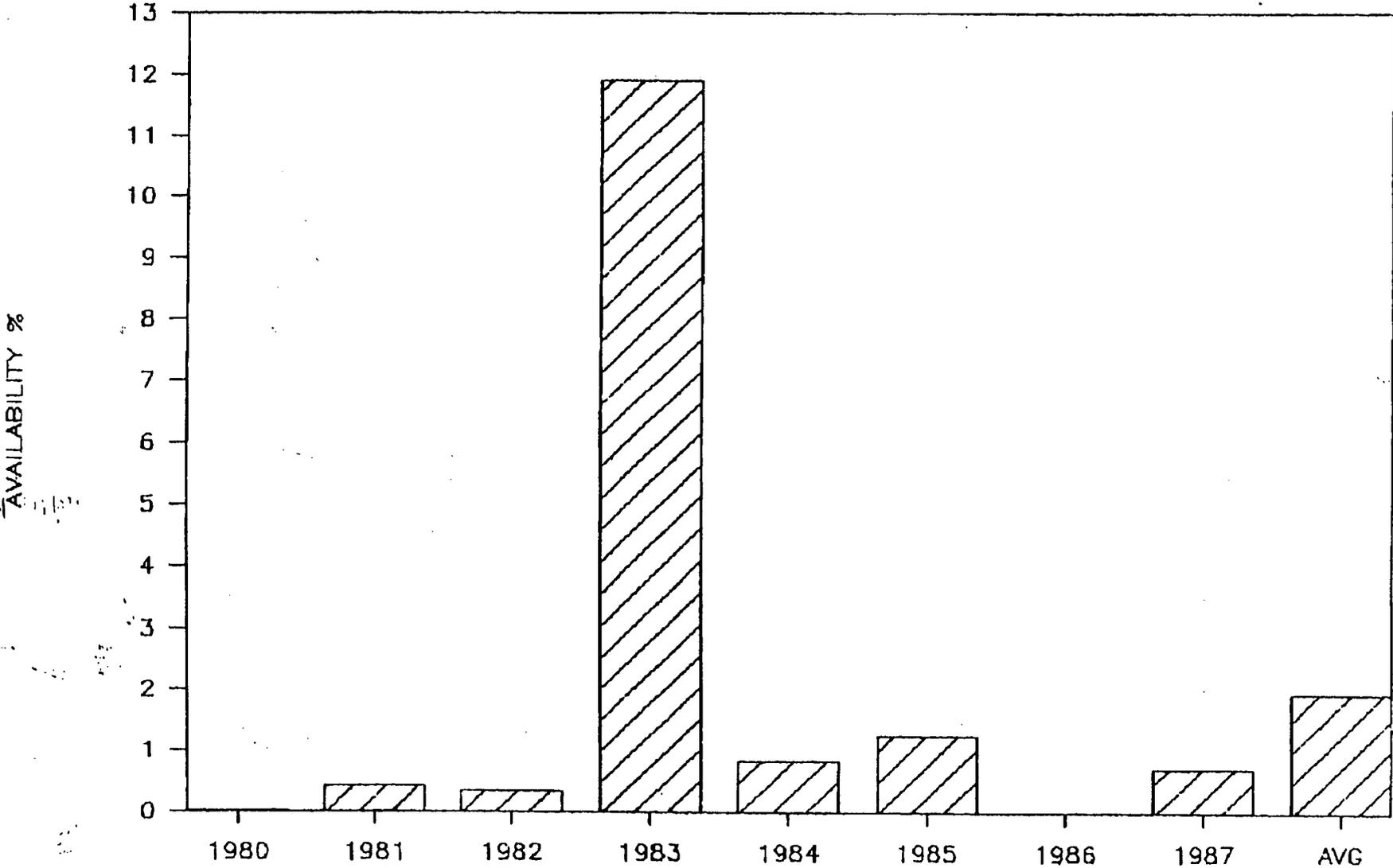
SUMMATION OF BOTH UNITS

	1980	1981	1982	1983	1984	1985	1986	1987	TOTAL
Number of Demands	601	613	519	683	697	536	584	631	4864
Number of Runhours	1301.8	758.2	595.8	1100	1126	723.7	665.7	888.7	7159.9
Number of Demand Failures	4	2	1	3	2	4	3	0	19
Number of Run Failures	0	1	0	0	1	1	0	0	3
Hrs Of Lockout Maintenance (single unit)	247.2	307.5	288.1	232.4	558.2	210.6	235.3	489.5	2568.8
Unavailability Due To Lockout (single unit)	2.82%	3.51%	3.29%	2.65%	6.37%	2.40%	2.69%	5.59%	3.67%
Hrs Of Lockout Maintenance (both units)	1.5	37.1	29.4	1042.1	73.8	109.4	0	62.4	1355.7
Unavailability Due To Lockout (both units)	0.02%	0.42%	0.34%	11.90%	0.84%	1.25%	0.00%	0.71%	1.93%

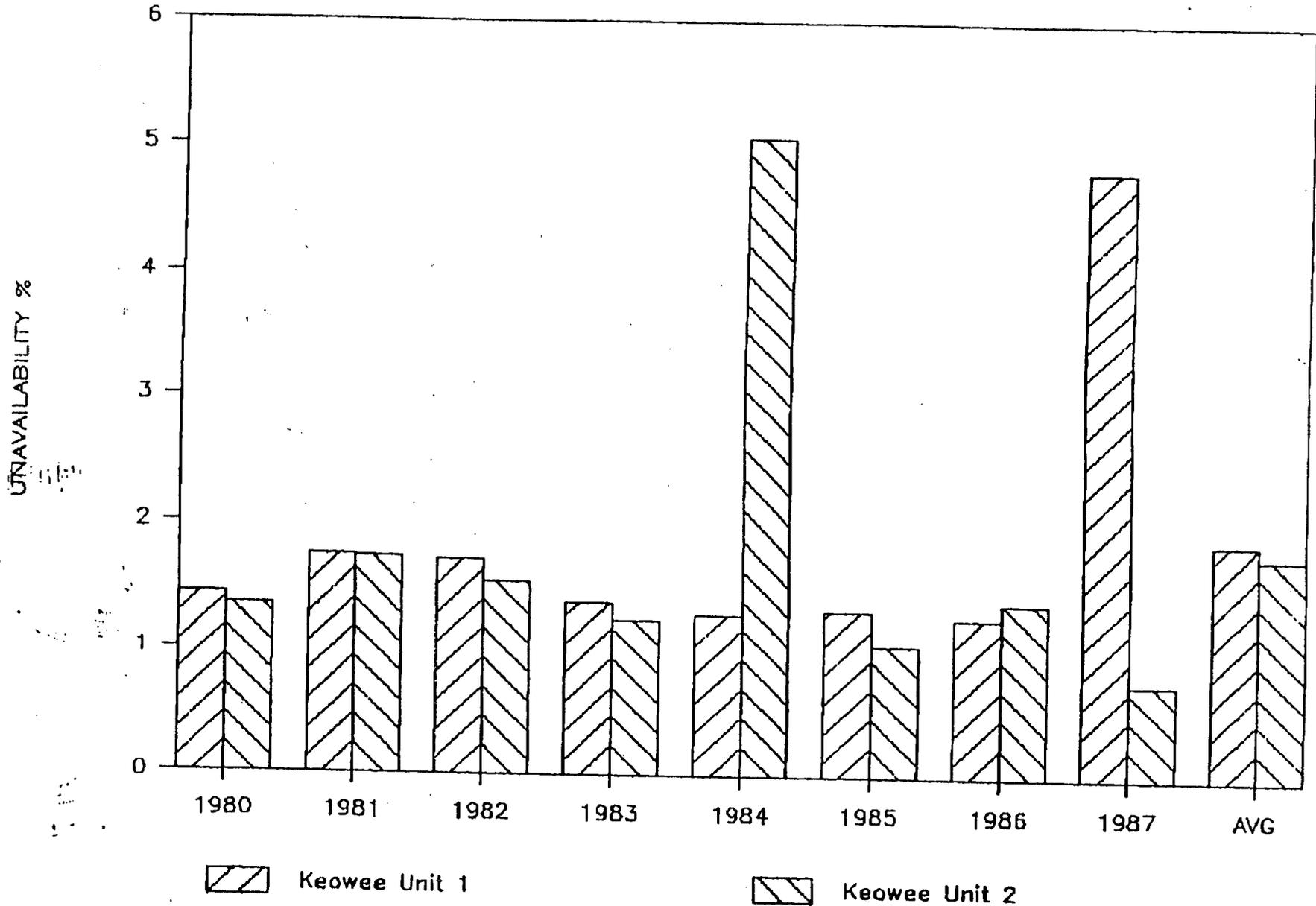
Note: Yearly Unavailability = Yearly Lockout Hrs / Hrs in Year  
 Total Unavailability = Total Lockout Hrs / Total Years

# BOTH UNITS IN LOCKOUT

SIMULTANEOUSLY

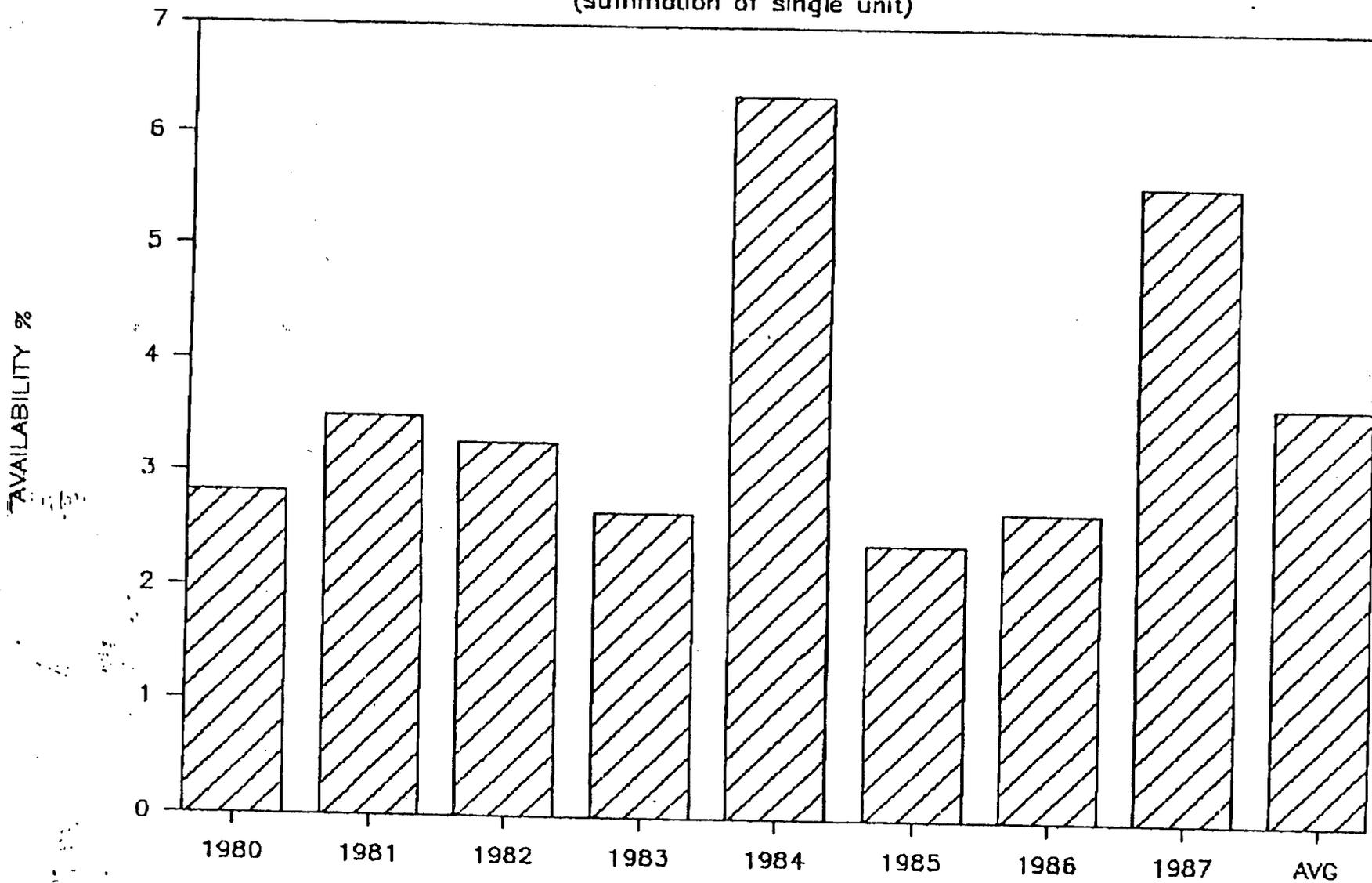


# SINGLE UNIT IN LOCKOUT



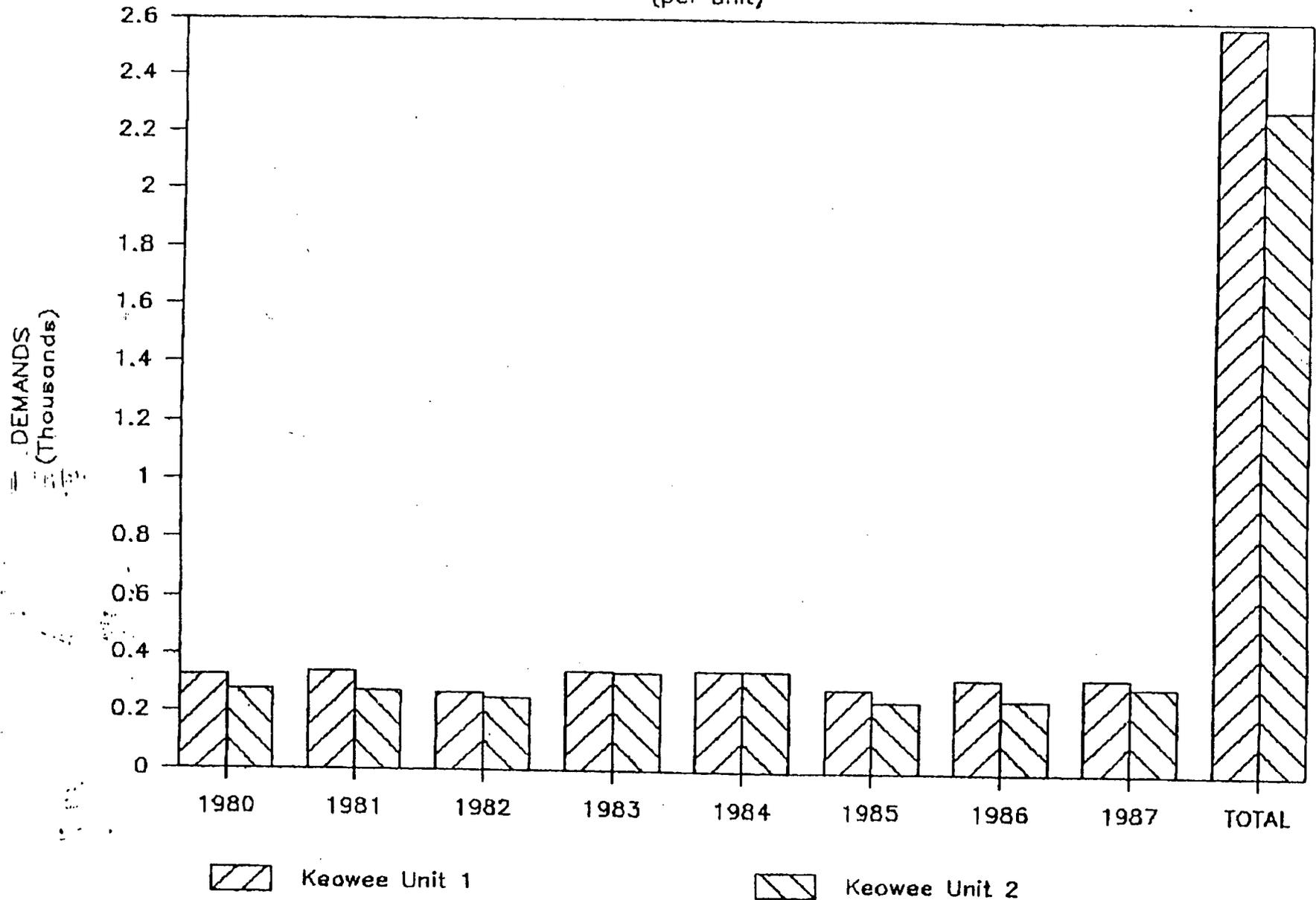
# EITHER UNIT IN LOCKOUT

(summation of single unit)



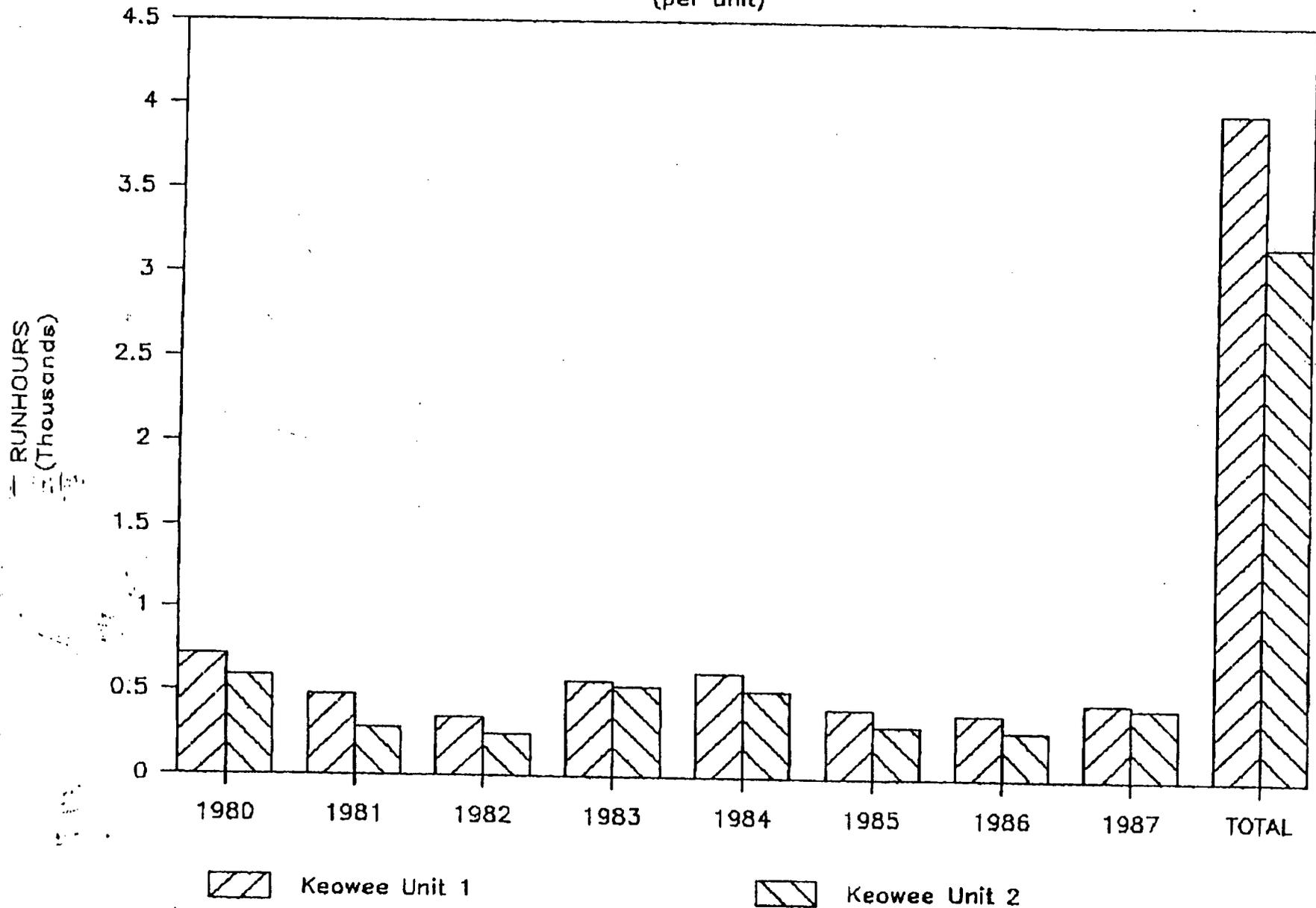
# NUMBER OF DEMANDS

(per unit)



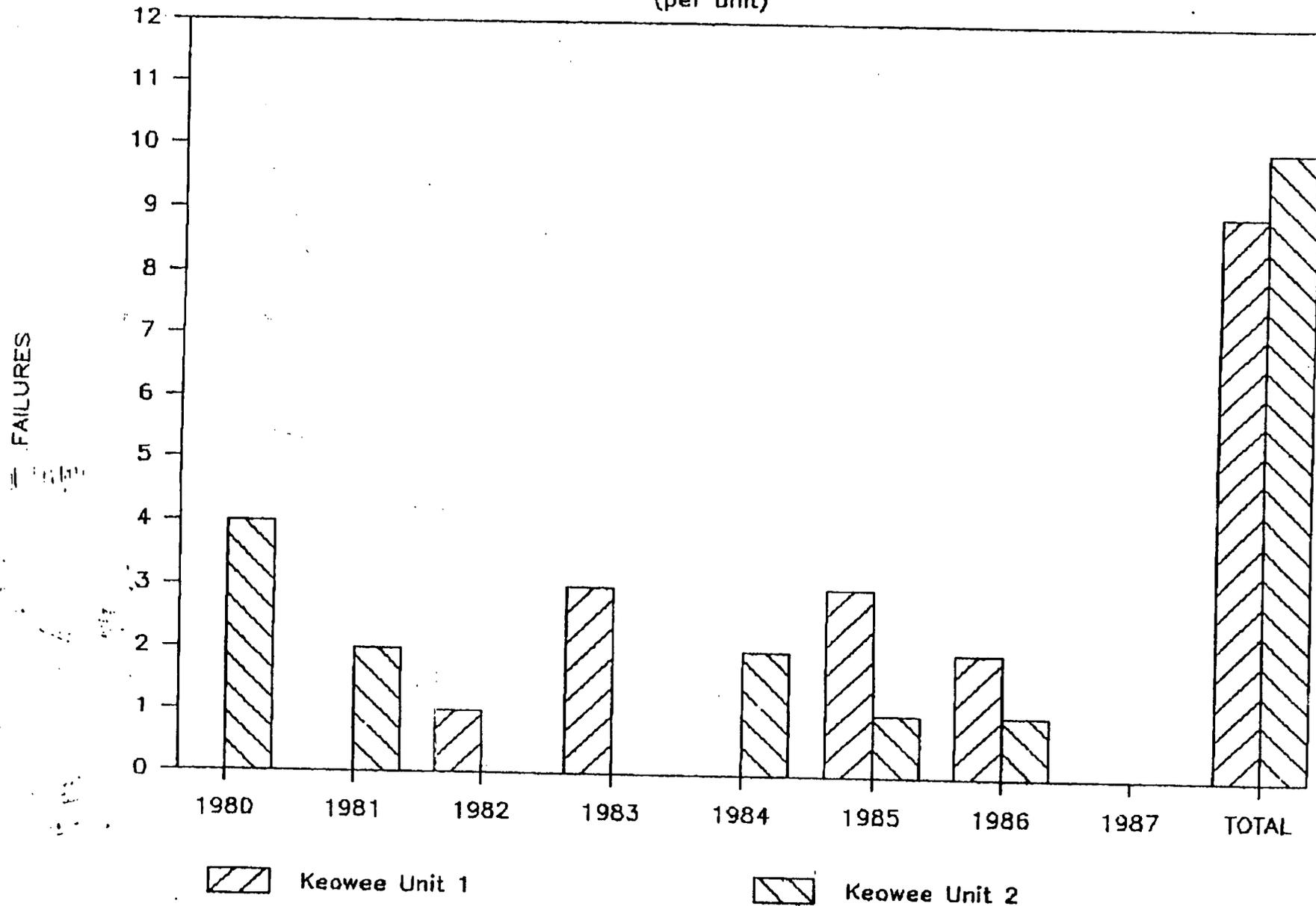
# NUMBER OF RUNHOURS

(per unit)



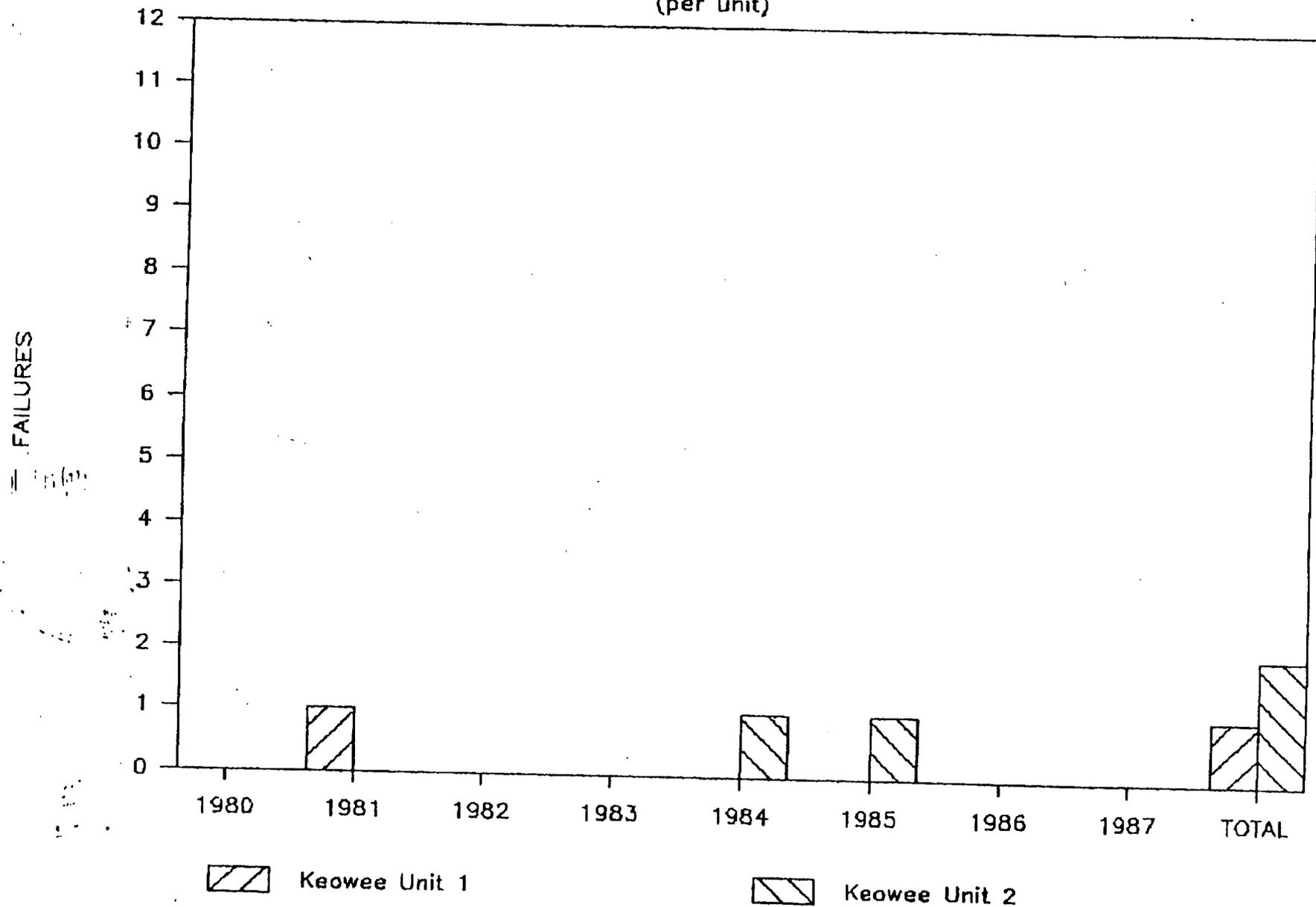
# NUMBER OF DEMAND FAILURES

(per unit)



# NUMBER OF RUN FAILURES

(per unit)



VIL

# Oconee Nuclear Station

## Problem Investigation Process

### Problem Investigation Form

PIP Serial No: 0-O95-0639  
MSE Serial No:

LER Serial No:  
Other Report:

#### I. Problem ID

Discovered Time/Date: 17:00 06/01/95      Occurred Time/Date:

Unit(s):	0	Status at Time Discovered:	Unit 1	Unit 2	Unit 3
		Mode:	1	1	1
		% Power:			

Unit Status Remarks:

System(s) Affected: EL      Electrical System  
                          K      Keowee

Affected Equipment:	Comp.	Manufacturer
<u>WMS Equipment ID No.</u>	<u>Code</u>	<u>Name</u>

Location of Problem - Bldg: KEO      Column Line:      Elev:

Location Remarks:  
Keowee Regulator/Exciter

Method Used to Discover Problem:  
KC-2023, Keowee Regulator Setting Analysis

Brief Problem Description:  
Keowee Emergency Start Procedure Acceptance Criterion incorrect.

Detail Problem Description:  
Recent conversations with Nuclear GO personnel involved in ONS emergency power path analyses have cast doubt on the adequacy of the Keowee voltage adjuster preset positions. The preset positions will determine what voltage the generator will comeup to during an automatic emergency start. The adjusters are currently calibrated for 13.8KV on the generator. The tolerance of the adjuster presets are field adjustable. Per conversations with the ESS regulator technician, experience indicates that the generator voltage can reasonably be expected to reach the designed preset voltage plus or minus 2%.

The dynamic analyses which ensures adequate voltage to ONS emergency power system loads (OSC-5701) used a terminal voltage of 13.8KV. A static analysis (OSC-2444) modeled a generator

# Oconee Nuclear Station

## Problem Investigation Process

### Problem Investigation Form

PIP Serial No: 0-O95-0639  
MSE Serial No:

LER Serial No:  
Other Report:

output voltage of 13.2KV. It was thought that the 13.2KV voltage should be considered the minimum allowable voltage, and voltage bands of 13.5 to 14.1KV were given to Operations to be incorporated into the applicable test and EOP procedures.

During efforts to define the allowable voltage band to identify the appropriate calibration settings for the adjusters, the engineer in GO was contacted, and expressed some reservations with allowing any no load voltage below 13.8KV due to marginally acceptable results of the OSC-5701 dynamic analysis.

Investigation of this problem revealed that the acceptance criterion for voltage in the Keowee emergency start test has been changed to 13.5KV. This should be changed back to 13.8KV.

Originated by: CESCHAEF Group: ESE Date: 06/01/95

Revised by: CESCHAEF Group: ESE Date: 06/01/95

Revised by: CESCHAEF Group: ESE Date: 06/02/95

Other Units/Components/Systems/Areas Affected (Y,N,U): N

Industry Plants Affected (Y,N,U):

Immediate Corrective Actions:

Nuclear GO was contacted to begin an analysis at the current minimum allowed voltage of 13.5KV

Originated by: CESCHAEF Group: ESE Date: 06/01/95

January 12, 1992

M. E. Bailey  
Electrical Engineering

Subject: Oconee Nuclear Station  
Pre-EDSFI SITA Audit  
DBA/LOOP Timing Licensing Basis

Section 5.8.3 of SITA 92-01 (ON) states that the audit team did not agree with the regulatory position taken regarding timing of LOCA/LOOP events. Further detail regarding the auditors concern are provided in the associated Request For Information (RFI), ONH-033 Accident and Seismic Event. The RFI asks for information to show that ONS can meet certain design requirements in the Unit 1 SER, AEC proposed GDC 44, and AEC question 4.1 from the PSAR recognizing that the ES signal may not be generated at  $t=0$  for events other than LBLOCA. The following information provides a general discussion of the ONS licensing basis with regard to LOOP timing and is followed by a specific response to each of the design requirements cited by RFI ONH-033.

A review of the Oconee PSAR, original FSAR, SER, current FSAR, and selected correspondence has been performed to identify the licensing basis for ONS with regard to the timing of LOOP events. Relevant quotes are attached. Based on this information the following conclusions can be drawn:

The original licensing basis is clear. All references to LOCA/LOOP are for the events to be "coincident" or "simultaneous". There is no specific requirement to evaluate LOOP at any other time during the event, nor is there any specific requirement to evaluate LOCA/LOOP to determine the most limiting time for LOOP. The LOCA/LOOP DBA evaluated (and accepted by the NRC) occurred simultaneously, e.g., the LOOP occurred on ES actuation. Note that the LOOP in and of itself is a DBA. Therefore, consideration of a LOOP at any time during a LOCA other than simultaneous with the ES actuation is beyond the original licensing basis.

The current licensing basis is contradictory. A specific assumption in the SBLOCA analysis is that LOOP occurs on reactor trip rather than simultaneous with the ES actuation. This assumption is conservative from a thermal-hydraulic perspective, however, it goes beyond the original licensing basis for the auxiliary power system. No additional information was identified which would contradict the conclusions of the operability evaluation for PIR 4-091-0074, or the description of this scenario within the Design Basis Event DBD. It is important to note that variation in LOOP timing, such as LBLOCA delayed LOOP, can invalidate ECCS timing assumptions for plants with EDGs. Further, Generic Issue 17, Loss of Off-Site Power Subsequent to a LOCA (addressed in NUREG 0933, Prioritization of Generic Safety Issues) drops consideration of the event due to low probability. The issue was also dismissed during Appendix K rulemaking in 1972 (ref NUREG/CR-4893 section 3.11.4). Based on this, one can conclude that the current licensing basis does not require consideration of LOOP at times other than simultaneous with LOCA.

The following design requirements were cited in the RFI; specific responses follow:

- 1) The Unit 1 SER states that for design purposes, there be no loss of function for the worst LOCA combined with seismic conditions, where that function is related to safety. The RFI notes that a seismic event will result in LOOP since offsite sources are not seismically qualified.

In the original ONS FSAR, upon which the SER is based, the worst case LOCA was considered to be the LBLOCA. The ES signal is effectively generated simultaneously with a LBLOCA. One can postulate seismic events causing LOOP at times other than simultaneous with the ES actuation. As discussed above, the LOCA/LOOP evaluated and accepted by the NRC occurred simultaneously, with no mention of the cause of the LOOP. Therefore, consideration of a LOOP (regardless of cause) at any time during a LOCA other than simultaneous with the ES actuation is beyond the licensing basis.

- 2) Proposed AEC GDC 44 specifies that the plant be designed to prevent fuel damage for all sizes of breaks in the reactor coolant pressure boundary. The RFI notes that PIR 4-091-0074 documents the concern that the ES signal may not be generated at  $t=0$  for SBLOCA.

The assumption in the SBLOCA analysis regarding LOOP timing provides conservative results from a thermal hydraulics perspective. However, it is inappropriate to extrapolate this assumption to be part of the licensing basis for the auxiliary power system since the LOOP occurred simultaneous with the ES actuation for the LOCA/LOOP DBA evaluated and accepted by the NRC.

- 3) The RFI states that AEC question 4.1 (included as a supplement to the PSAR) asks Duke to show that the emergency power system be able to withstand an accident (non-specific), simultaneous with a LOOP, and a single failure.

In the response to the AEC question, the only discussion of LOOP timing is the consideration of the simultaneous LOOP. However, it is inappropriate to attempt to draw conclusions from this response since the discussion of selection and transfer to emergency power sources describes power sources and priorities which were never implemented in the system design. With regard to consideration of events other than LBLOCA with variations in LOOP timing, given dismissal of LOCA delayed LOOP (GI 17) by NUREG-0933 and SGTR delayed LOOP in NUREG/CR-4893 on the basis of low probability it is inappropriate to consider other ANS Condition IV DBAs with variations in LOOP timing.

Therefore, based on the above, the licensing basis for the auxiliary power system does not include consideration of LOOP at times other than simultaneous ES actuation.

In order to assure that the SBLOCA/LOOP sequence identified is not safety

significant, the Severe Accident Analysis Group analyzed LOCA/LOOP sequences which could cause the standby bus to be overloaded. This analysis concluded that these sequences are highly improbable. Further, the frequency of such events is much less than the estimated frequency of a number of other events (core melt events, extreme external initiator events, etc.) for which the plant is not required nor known to have adequate protection capability.

M. E. Patrick  
Compliance Manager



By: Phillip J. North, Nuclear Production Engineer  
Regulatory Compliance

xc: H. B. Barron, ONO1VP  
J. M. Davis, ONO1VP  
R. L. Sweigart, ONO101  
B. L. Peele, ONO1VP  
R. L. Dobson, ONO2EE  
B. J. Dolan, ONO2ME  
D. M. Jamil, ONO2EE  
D. B. Coyle, ONO1SE  
R. L. Gill, EC050  
K. S. Canady, EC08H  
G. B. Swindlehurst, EC08H  
P. M. Abraham, EC08I  
A. V. Carr, PB05E  
File

PSAR Supplement 2, question 4.1:

Please discuss the reliability of those power generation sources and associated circuitry which will provide emergency power in the event of an accident and simultaneous loss of the external grid.

The the only discussion of LOOP timing is the consideration of the simultaneous LOOP. In the discussion of transfer logic (p4.1-14) "Each of the redundant logic systems is arranged to monitor all power sources continuously through redundant sensors, thereby allowing immediate selection of the first available priority power source. Upon selection and transfer to this emergency power source, the logic will lock into this source and stop the automatic sequence. If this source is lost, the sequence will automatically be initiated and select the next available source. If a preferred power source becomes available during the time the automatic sequence is stopped, the operator may make a manual transfer to this source."

Note that the available sources and the priority of selection differs significantly from that which was actually licensed.

Original FSAR, Chapter 6:

6.1.2.9 (p 6-8) The single failure analysis presented in Table 6-2 "was based on the assumption that a major LOCA had occurred and coincidentally an additional malfunction or failure occurred in the engineered safeguards system. For example, the analysis included malfunctions or failures such as electrical circuit" failures...

Original FSAR, Chapter 8:

8.2.3.1(c) (p8-12) The Keowee units "are available to carry load within 23 sec upon occurrence of any of the following abnormal incidents: 1) Engineered safeguards required; 2) System network undervoltage; 3) system network underfrequency."

8.2.3.2 (p8-13) "The engineered safeguards auxiliaries and RPS are arranged so that a failure of any single bus section does not prevent the respective systems from fulfilling their protective functions." The preferred sequence of transfer to startup then transfer to standby is then described.

8.2.3.3 (p8-14c) "In the event of an accident requiring engineered safeguards, and the simultaneous loss of the complete external transmission network; power is provided from either or both of the two on-site Keowee generating units"

8.2.3.3C (p8-17) "The redundant transfer logic will seek the most available source of power and when it becomes available close into it. If the source is then subsequently lost, the switching logic and equipment

will transfer to the other source automatically."

Original FSAR, Chapter 14:

No mention is made of specific single failure assumptions or LOCA/LOOP. Reference is made to Chapter 6 for ECCS system description.

Oconee SER:

The SER concludes that ECCS is acceptable and will provide adequate protection for any LOCA, and that the onsite power system is acceptable.

Current FSAR:

8.3.1 (p8-22) Only the simultaneous accident and LOOP is evaluated.

15.14.3.3.6 Worst case single failures are identified. No discussion of the timing of the single failures is provided. The B&W SBLOCA Topical is referenced which includes an assumption that LOOP occurs on reactor trip (rather than ES).

## 7.0 RESULTS OF THE SIMULATION

### 7.1 CASE RESULTS

#### Cases 1H, 1L, 2H and 2L: ( KH90.PL, KL90.PL, KH75.PL, and KL75.PL )

These cases were simulated to determine the time when the frequency would come down to 1.17 pu, thus allowing the 27E relays to start the reset process. The reset time can be obtained by adding an additional 4 seconds. Based on Figure J1 in Appendix J, the reset times for these cases are:

Case 1L, 90 MW LR @ 113' - 24.2 seconds following a LOOP

Case 1H, 90 MW LR @ 140' - 19.7 seconds following a LOOP

Case 2L, 75 MW LR @ 113' - 21.0 seconds following a LOOP

Case 2H, 75 MW LR @ 140' - 17.2 seconds following a LOOP

#### Case 3L: ( KL75L1.PL )

This case was simulated to provide a basis for the scenario where the LOCA unit would be transferred to the Underground Unit 11 seconds following the event. The overpath circuit was used to simulate this case because the underground circuit was not yet created and the results from using the overhead should be a good indicator as how the Underground Unit would perform. At 11 second, following a 75 MW load rejection, the frequency of the Underground Unit would be the same as the overhead path unit's. As a result, some of the safety motors are expected to trip on overcurrent. Figure J2 in Appendix J shows the starting current and time for Reactor Building Spray Pump Motor, 5.08 pu for 370 cy. Based on the overcurrent relay setting shown in Attachment 5, this motor is expected to trip, hence Case 3L is not acceptable.

#### Case 4L: (KL75R4.PL)

The result of this case shows that the startup bus does not recover high enough for the 27E relays to reset. Figure J3 in Appendix J shows the startup bus voltages.

#### Cases 5H, 6L and 7L: (KH00L123.PL, KL75L231.PL, and KL75L123.PL)

For these cases the voltage and frequency recoveries are acceptable. However, detailed analyses of the motor performances are needed. The following table provides such details. The Table includes, for the most parts, loads and buses for Unit 1 which should be the worst case because of higher LOCA loads. For Cases 5H and 7L, loads are energized at t=180 cy and t=1320 cy, respectively. For Case 6L, Units 2&3 are connected at t=1320 cy and Unit 1 at ten seconds later, t=1920 cy. In Case 6L, only the effect of the second load application. Unit 1 LOCA, is examined; Case 7L should envelop the first load application ( 2-Unit LOOP). }

#### 4.0 CONCLUSION

Based on the results of various cases being analyzed, the Keowee units with existing control logic can be considered as viable emergency sources for an Oconee three-unit LOOP concurrent with a single unit LOCA scenario only if the conditions given in either 4.1 or 4.2 are satisfied. In addition, it was observed that the setting of the overcurrent relays in some cases could be increased and still be below the motor thermal damage curve. Thus, the setting of the 4 KV motor overcurrent relays should be reviewed to determine if the settings can be increased allowing longer motor starting times.

4.1 The Keowee Underground Unit (KUG) must not generate to the grid, and the Keowee Overhead Unit (KOH) must generate no more than 75 MW<sup>1</sup> to the grid. If the KOH separates from the grid, it must not be reconnected to the grid before all of the reactor coolant pump motors at Oconee have been tripped off.

4.2 Both KUG and KOH can generate up to 75 MW<sup>1</sup> to the grid if the KUG control system is modified such that the KUG will only be reconnected the underground circuit following a load rejection when the unit has decreased in speed to 1.10 pu or less.

---

<sup>1</sup> 90 MW if the difference between the headwater and the tailrace levels is 125' or greater