

Safety Evaluation Report

NUREG-0308
Suppl. No. 1

U. S. Nuclear
Regulatory Commission

related to operation of
Arkansas Nuclear One, Unit 2

Office of Nuclear
Reactor Regulation

Arkansas Power and Light Company

Docket No. 50-368

June 1978

Supplement No. 1

— NOTICE —

THE ATTACHED FILES ARE OFFICIAL RECORDS OF THE DIVISION OF DOCUMENT CONTROL. THEY HAVE BEEN CHARGED TO YOU FOR A LIMITED TIME PERIOD AND MUST BE RETURNED TO THE RECORDS FACILITY BRANCH 016. PLEASE DO NOT SEND DOCUMENTS CHARGED OUT THROUGH THE MAIL. REMOVAL OF ANY PAGE(S) FROM DOCUMENT FOR REPRODUCTION MUST BE REFERRED TO FILE PERSONNEL.

DEADLINE RETURN DATE

50-368

w/ Hr. 7/12/78

RETURN TO REGULATORY CENTER

RECORDS FACILITY BRANCH

Available from
National Technical Information Service
Springfield, Virginia 22161
Price: Printed Copy \$6.00; Microfiche \$3.00

The price of this document for requesters outside
of the North American Continent can be obtained
from the National Technical Information Service.

Supplement No. 1 to
NUREG-0308

SUPPLEMENT NO. 1
TO THE
SAFETY EVALUATION REPORT

OFFICE OF NUCLEAR REACTOR REGULATION
U.S. NUCLEAR REGULATORY COMMISSION

IN THE MATTER OF

ARKANSAS POWER AND LIGHT COMPANY
ARKANSAS NUCLEAR ONE - UNIT 2
DOCKET NO. 50-368

Docket # 50-368
Control # _____
Date 7/12/78 of Document
LABORATORY DOCKET FILE

1970-1971
1972-1973
1974-1975
1976-1977
1978-1979
1980-1981
1982-1983
1984-1985
1986-1987
1988-1989
1990-1991
1992-1993
1994-1995
1996-1997
1998-1999
2000-2001
2002-2003
2004-2005
2006-2007
2008-2009
2010-2011
2012-2013
2014-2015
2016-2017
2018-2019
2020-2021
2022-2023
2024-2025

TABLE OF CONTENTS

	<u>PAGE</u>
1.0 INTRODUCTION AND GENERAL DISCUSSION.....	1-1
1.1 Introduction.....	1-1
1.6 Summary of Outstanding Review Items.....	1-1
1.7 Generic Issues.....	1-5
2.0 SITE CHARACTERISTICS.....	2-1
2.1 Geography and Demography.....	2-1
4.0 REACTOR.....	4-1
4.4 Thermal and Hydraulic Design.....	4-1
5.0 REACTOR COOLANT SYSTEM.....	5-1
5.7 Overpressure Protection.....	5-1
5.8 Loose Parts Monitoring.....	5-6
7.0 INSTRUMENTATION AND CONTROLS.....	7-1
7.1 General.....	7-1
7.2 Reactor Trip System.....	7-1
7.2.2 Reactor Trip System - Hardwired Analog Portion.....	7-1
7.2.3 Reactor Trip System - Digital Computer Portion.....	7-2
7.3 Engineered Safety Features Systems.....	7-6
7.3.2 Engineered Safety Features Actuation and Basic Logic.....	7-6
7.6 Other Systems Required for Safety.....	7-6
7.6.3 Safety-Related Fluid Systems.....	7-6
7.6.4 Reactor Coolant Pump Coastdown Capabilities.....	7-7

TABLE OF CONTENTS (Continued)

	<u>PAGE</u>
14.0 INITIAL TESTS AND OPERATIONS.....	14-1
15.0 ACCIDENT ANALYSES.....	15-1
15.4 Postulated Accidents.....	15-1
15.4.7 Fuel Handling Accident.....	15-1

APPENDICES

	<u>PAGE</u>
APPENDIX A - SUPPLEMENT TO THE CHRONOLOGY OF RADIOLOGICAL SAFETY REVIEW.....	A-1
APPENDIX B - SUPPLEMENT TO THE BIBLIOGRAPHY FOR THE ANO-2 SAFETY EVALUATION REPORT.....	B-1
APPENDIX D - SUPPLEMENT TO THE EVALUATION OF THE CORE PROTECTION CALCULATOR SYSTEM.....	D-1



1.0 INTRODUCTION AND GENERAL DESCRIPTION OF THE PLANT

1.1 Introduction

On November 11, 1977 the Nuclear Regulatory Commission (Commission) issued its Safety Evaluation Report regarding the application for a license to operate the Arkansas Nuclear One-Unit 2 (ANO-2) facility. The application was filed by the Arkansas Power and Light Company (applicant).

Since preparation of the Safety Evaluation Report, we have received and reviewed Amendment No. 44 to the Final Safety Analysis Report and additional documents associated with the application, held a number of meetings with the applicant and met with the Advisory Committee on Reactor Safeguards. These events and documents are identified in Appendix A to this supplement.

This supplement, Supplement No. 1 to the Safety Evaluation Report, provides (1) our evaluation of additional information received from the applicant since preparation of the Safety Evaluation Report regarding previously identified outstanding review items, and (2) a listing of additional or revised information related to new issues that have arisen since the preparation of the Safety Evaluation Report.

Each section of this supplement is numbered and titled to correspond to the sections of the Safety Evaluation Report that have been affected by our additional evaluation, and except where specifically noted, does not replace the corresponding section of the Safety Evaluation Report. Appendix A is a continuation of the chronology of principal events that have occurred during the safety review. Appendix B lists additional documents used in the supplemental review.

Upon favorable completion and resolution of the outstanding matters described in this supplement, we conclude that the plant can be operated without endangering the health and safety of the public.

1.6 Summary of Outstanding Review Items

Items previously identified as outstanding have been resolved since publication of the Safety Evaluation Report as indicated below.

In Section 1.6 of the Safety Evaluation Report, we identified 19 items related to the overall plant design that were outstanding because additional information was

required from the applicant or because the staff had not completed its review of recently submitted information. We also identified 22 staff positions relating to the core protection calculation system (CPCS) design that were outstanding because additional information was required from the applicant, because the staff had not completed its review of recently submitted information, or because the staff had established positions with which the applicant disagreed.

Since preparation of the Safety Evaluation Report was completed, four of the nineteen outstanding items described in Section 1.6 have been resolved. In addition, three of the four other items that were identified in the Safety Evaluation Report but not listed in Section 1.6 have been resolved. These four additional items are identified by an asterisk in the following list of items. However, since preparation of the Safety Evaluation Report, we have identified seven additional items which require resolution for the ANO-2 plant prior to the issuance of the operating license. Although the staff has not yet prepared a safety evaluation on these matters for inclusion in this supplement to the Safety Evaluation Report, these items have been discussed at the February 9, 1978 meeting of the Advisory Committee on Reactor Safeguards. These seven items include (1) verification of fuel assembly burnable poison rod design parameters, (2) A surveillance plan to periodically measure the reactivity worth of the control element assemblies, (3) control element assembly guide tube integrity, (4) steam generator tube support plate integrity, (5) fire protection evaluation, (6) emergency plan deficiencies and (7) pre-operational tests for reactor coolant piping vibration measurements and the loss of offsite power test. We are pursuing the resolution of these issues with the applicant and will report our evaluations in a supplement to this report.

Therefore, with the designation of the offsite grid stability evaluation as an item that we will require to be resolved prior to the issuance of the operating license the number of unresolved items relating to the overall plant design stands at 24.

Since preparation of the Safety Evaluation Report was completed, 12 of the 22 outstanding staff positions relating to the CPCS have been resolved. Three additional positions have been acceptably resolved for the issuance of the operating license; however, verification testing programs to be executed in the startup phase of plant operations are required to be acceptably completed in support of the final resolution of these positions. Seven positions remain outstanding because additional information is required from the applicant or because the staff has not completed its review of recently submitted information.

The current status of all review items discussed above and the sections of Supplement No. 1 to the Safety Evaluation Report that provide our evaluation of each item are tabulated below. Those items for which the status is unchanged are described in the section of the Safety Evaluation Report referenced.

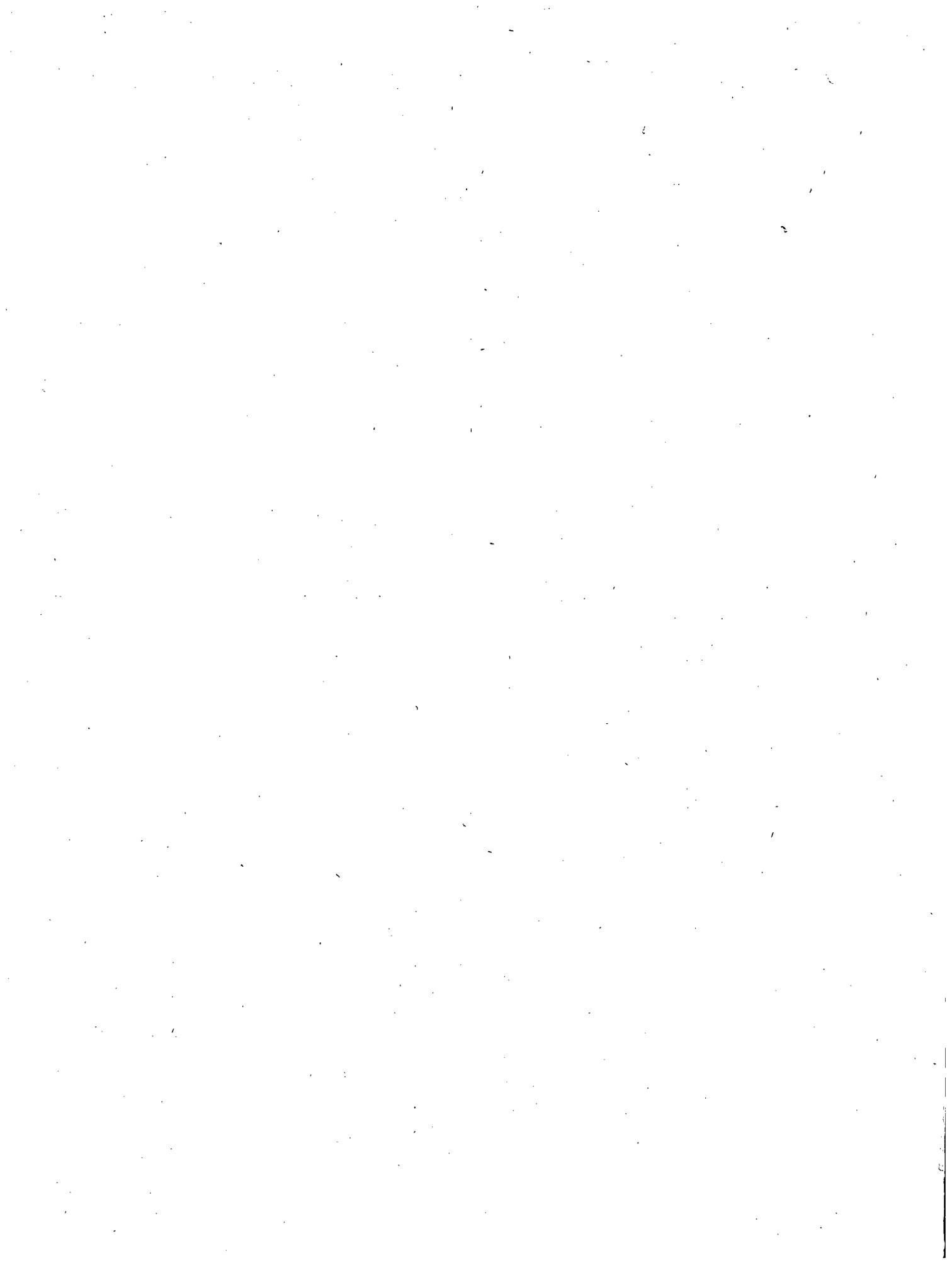
<u>Report Section</u>	<u>Item</u>	<u>Status</u>
2.1	Low Population Zone Radius	Resolved pending documentation
3.10	Seismic Qualification of Safety-Related Instrumentation	Additional information was recently submitted
3.11	Environmental Qualification of Safety-Related Instrumentation	Additional information required
4.4	Rod Bow Penalty on DNBR*	Resolved
5.7	Overpressure Protection - Interim Measures	Resolved
5.8	Loose Parts Monitoring*	Resolved pending documentation
6.2.1	Main Steam Line Break Mass and Energy Releases	Additional information was recently submitted
6.2.1	Environmental Qualifications for Safety-Related Equipment for Main Steam Line Break Inside Containment	Additional information was recently submitted
6.2.6	Containment Leakage Testing Program	Additional information required
6.3.3	Evaluation of Emergency Core Cooling System Performance	Additional information required
6.3.4	Emergency Core Cooling System Operation in Recirculation Mode	Additional information was recently submitted
7.1	Verification of Implementation of Instrumentation and Control Systems Design	Additional information was recently submitted
7.2.2, 7.3.3 and 7.3.6	Input Fault and Surge Testing for Power Supplies	Additional information required

<u>Report Section</u>	<u>Item</u>	<u>Status</u>
7.2.3	Core Protection Calculator System	
	The seven outstanding core protection calculator system staff positions, as discussed in Section 7.2.3 listed in Table 7.1 of this report, are listed in accordance with the position's number which has been used to identify the position in previous documentation. Indicated section numbers refer to the applicable section of Appendix D to this report.	
	(4) CEAC separation criteria (Section 4.1.4)	
	(14) Seismic qualifications. This is redundant to item 3.10 of this outstanding item list (Section 4.2.5).	
	(15) Limit magnitude of change allowed for addressable constants (Section 3.11).	
	(18) Integrated system burn in qualification test (Section 4.1.4)	
	(19) Qualification of software change procedures (Section 4.4)	
	(20) Data links to plant computer system (Section 4.2.3).	
	(26) Qualification of optical isolator device (Section 4.1.4).	
7.5.1	Accident and Post-Accident Monitoring	Additional information required
7.6.3	Redundant Valve Position Indication	Additional information required
7.6.4	Reactor Coolant Pump Coastdown	Resolved
7.9.4	Separation Criteria For Conduits	Additional information was recently submitted
8.2	Offsite Grid Stability	Additional information was recently submitted

<u>Report Section</u>	<u>Item</u>	<u>Status</u>
10.6	Feedwater Hammer in Steam Generator*	Additional information was recently submitted
14.0	Initial Tests and Operations (Rod drop time testing)	Resolved pending documentation
15.4.2	CESEC Code Verification Program for reactor coolant pump seizure analysis.	Additional information required
15.4.4	Main Steam Line Break Analysis	Additional information required
15.4.7	Fuel Handling Accident in Containment*	Resolved
20.0	Financial Qualifications	Additional information has been submitted

1.7 Generic Issues

The item number four identified in Section 1.7 of the Safety Evaluation Report as offsite grid stability is required to be resolved prior to the issuance of an operating license and is included in Section 1.6 of this report.



2.0 SITE CHARACTERISTICS

2.1 Geography and Demography

In the Safety Evaluation Report we stated that, based on projections of the growth of the City of Russellville and its surroundings, it should be considered the population center as defined in 10 CFR Part 100. We also stated that we believe a low population zone radius of 3200 meters (two miles) would be appropriate for the ANO-2 plant. The applicant did not agree with this position, and we agreed that additional information submitted by the applicant would be reviewed to make a final determination on this matter. We have reviewed the information submitted by the applicant as well as information independently obtained and conclude that the minimum population center distance for the ANO-2 site should not be greater than about 5600 meters (3.5 miles) and that the corresponding low population zone distance should be no greater than 4200 meters (2.6 miles). The bases for our conclusion are set forth below.

The present population of the City of Russellville, as determined by a special census conducted in 1975, is about 14,000. The average population density in that city is about 2000 people per square mile based on the present area within the city limits of about seven square miles. Figure 2.1 shows the present western boundary of the City of Russellville and defines the type of zoning for the illustrated areas within the city limits. The selection of the distance from the reactor to the nearest boundary of a densely populated center is to be based on considerations of the population distribution as set forth in 10 CFR Part 100, Section 100.11.3(a). The applicant's submittal proposed establishment of the nearest boundary at Point B on Figure 2.1. The staff concluded, as described below, that there is, or will be, significant concentrations of people closer to the reactor. The "Russellville Zoning Ordinance," dated August 10, 1976, defines an R-1 zoning district as "single family residential" with a minimum lot area of 9600 square feet for single family residences and 20,000 square feet for churches. Other permitted uses are schools, parks, playgrounds, recreational buildings, and accessory buildings.

The Russellville Planning Document, states that in 1970 there were 3.2 persons per household, but assumes that in the future there will be 2.7 persons per dwelling unit. The Russellville Planning Document further indicates that in future subdivision design, 25 percent of the gross area will be devoted to streets and rights-of-way.

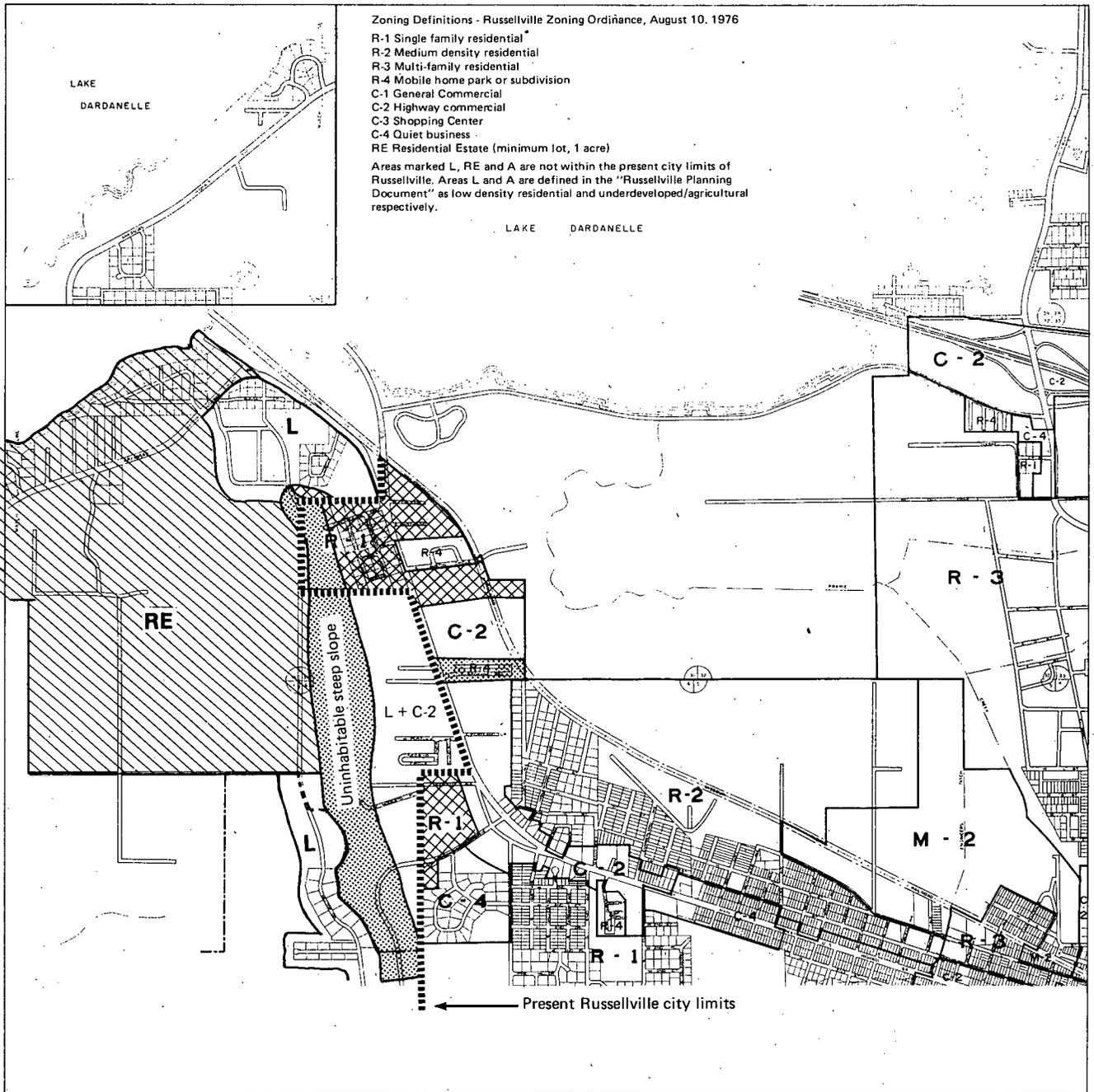


Figure 2.1

A minimum lot size of 9600 square feet would permit a maximum average of 4-1/2 dwelling units per acre, or a total of 12 persons per acre in an R-1 zoning district based on the 2.7 persons per unit. Twelve persons per acre is equivalent to 7680 persons per square mile. If it is assumed that 50 percent of the gross area is devoted to dwelling units to allow for the other permitted uses, an R-1 zoning district could have a density of six persons per acre or about 3800 people per square mile. Thus, the R-1 zoning districts on the western edge of Russellville, as shown in Figure 2.1, when fully developed, may have a population density equal to or greater than the average population density of the City of Russellville.

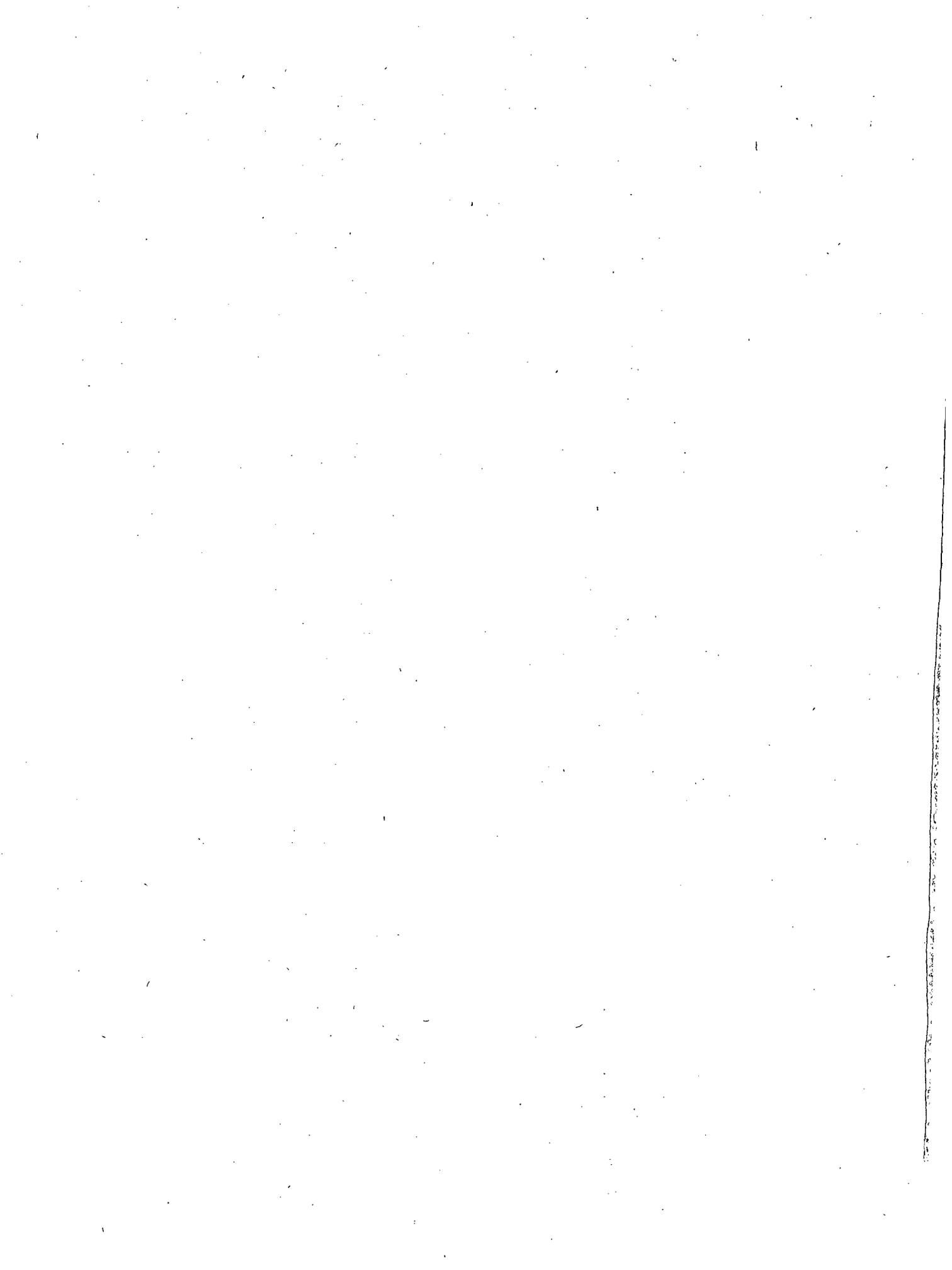
Since the areas west of the city limits are not subject to the Russellville Zoning Ordinance, they are not formally zoned at this time. The areas marked "L" are defined in the Russellville Planning Document as "low density residential." These areas could be zoned wholly or partially R-1 if annexation attempts are successful. Zoning districts classified as RE are presently limited by the zoning ordinance to minimum lots of one acre in size. The area marked RE (residential estate) west of the city limits, if fully developed, would have a population density of about 864 people per square mile if that zoning classification is retained, and if the same 50 percent of gross area is assumed for dwelling units. This density is less than 25 percent of the density of 3800 people per square mile for the R-1 zoning district as calculated above.

The applicant's submittal proposed establishment of the population center distance at Point B on Figure 2.1 which is about four miles from the plant site. As discussed above, establishment of the population center distance at that point would exclude from the population center areas in which the population density is equal to or greater than the average density of the population center itself. We can find no basis for concluding that such a proposal would meet the intent of 10 CFR Part 100 for determination of population center distance.

Based on the above considerations, we conclude that the boundary of the population center, Russellville, should be established at the nearest boundary of the R-1 zoning district at the western edge of the city since it marks a clear delineation between the population density of the city and the surrounding areas. This point is identified as Point A on Figure 2.1, and is about 5600 meters (3.5 miles) from the plant site. The corresponding low population zone radius is 4200 meters (2.6 miles).

The applicant has recently stated in a meeting held with the staff on January 25 and 26, 1977 that they planned not to pursue justification of a low population zone radius of greater than this 2.6 mile distance and indicated that they would amend the ANO-2 application to reflect the 2.6 mile low population zone radius.

Therefore, we consider this matter resolved pending documentation of the 2.6 mile low population zone radius in the ANO-2 license application.



4.0 REACTOR

4.4 Thermal and Hydraulic Design

In Section 4.4 of our Safety Evaluation Report, we stated that we were in the process of developing criteria for evaluating the effect of rod bowing on the departure from nucleate boiling ratio for application to Combustion Engineering 16x16 fuel assemblies. Our development of the rod bow penalty for ANO-2 and the bases for this penalty are discussed below.

ANO-2 is the lead plant with Combustion Engineering 16x16 fuel; therefore, there is no data base for direct evaluation of rod bowing as a function of burnup. Consequently, rod bow measurements on 14x14 fuel have been extrapolated, by the staff, to 16x16 fuel with methods which are generally conservative. This extrapolation was based on methods described in the staff's revised interim evaluation for rod bowing and combines the Combustion Engineering, Inc., data on the effect of rod bow on departure from nucleate boiling with rod bow magnitude versus exposure. Credit has been given for thermal margin due to a multiplier of 1.05 on the hot channel enthalpy rise used to account for pitch reduction due to manufacturing tolerances. The resultant reduction in departure from nucleate boiling ratio due to rod bow is given by:

<u>Burnup*</u>	<u>Departure From Nucleate Boiling Ratio Penalty (points)**</u>
0-2.1	0
2.1-5	4.0
5-10	5.9
10-15	8.8
15-20	11.4
20-25	13.6
25-30	15.6
30-35	17.4

*In units of Giga watt days per metric ton of uranium.

**Points subtracted from a departure from nucleate boiling ratio value. For example, a penalty of 4.0 points subtracted from 1.34 would result in a penalized value of 1.30.

The thermal margin reduction shown above will be accounted for in the technical specifications.

The staff will work with Combustion Engineering, Inc., to provide guidance on a generic method which could more accurately describe rod bowing and its effect on departure from nucleate boiling limits. It is very likely that reanalysis along with rod bow measurements at the end of the first cycle of operation could significantly reduce the penalty.

5.0 REACTOR COOLANT SYSTEM

5.7 Overpressure Protection

In Section 5.7 of our Safety Evaluation Report, we noted that there have been several incidents of reactor vessel overpressurization during startup and shutdown operations in which the limits of 10 CFR Part 50, Appendix G, "Fracture Toughness Requirements," were exceeded. We stated that we had requested additional information from the applicant describing both the short-term and long-term measures to acceptably minimize the probability and consequences of such overpressurization incidents.

The applicant has submitted a plant-specific analysis in support of the proposed reactor vessel overpressure mitigating system for ANO-2. Our review of all information submitted by the applicant in support of the proposed overpressure mitigating system is complete except for items noted below related to the long term program.

The basic design criterion is that the mitigating system will prevent reactor vessel pressures in excess of those allowed by Appendix G. Specific criteria for system performance are:

- (1) Operator action: no credit can be taken for operator action for ten minutes after the initiation of a transient.
- (2) Single failure: the system must be designed to relieve the pressure transients given a single failure in addition to the event that initiated the pressure transient.
- (3) Testability: the system must be testable on a periodic basis.
- (4) Seismic and IEEE Standard 279 criteria: the system is required to meet seismic Category I and IEEE Standard 279 criteria. The basic objective is that the system should not be vulnerable to a common failure that would both initiate a pressure transient and disable the overpressure mitigating system. Such events as loss of instrument air and loss of offsite power are considered.

The staff also required instrumentation which monitors the position of the pressurizer relief valve isolation valves, in conjunction with the system pressure, to assure that the overpressure mitigating system is properly aligned for shutdown conditions.

The incidents that have occurred to date have been the result of operator errors or equipment failures. Two varieties of pressure transients can be identified: a mass input type from charging pumps, safety injection pumps, and safety injection accumulators; and a heat addition type which causes thermal expansion from sources such as steam generators or decay heat.

The applicant evaluated the results of pressure transients due to (1) a reactor coolant system/steam generator secondary side temperature differential of 100 degrees Fahrenheit with the startup of a reactor coolant pump, (2) inadvertent safety injection with two high pressure safety injection pumps coupled with inadvertent injection of three charging pumps, (3) inadvertent injection with up to two charging pumps with no letdown flow available, (4) shutdown cooling system isolation at one percent decay heat, (5) inadvertent injection with one high pressure safety injection pump, and (6) inadvertent actuation of the pressurizer heaters. In their analysis, the applicant conservatively assumed that the reactor coolant system was water-solid, that no letdown path was available, that there was no sensible heat absorption by the reactor coolant system component metal mass, that reactor coolant system boundaries were fixed with no expansion, and that the reactor coolant system was at 300 pounds per square inch absolute, the highest pressure allowable for shutdown cooling. The fastest pressure increase was achieved by the inadvertent actuation of the safety injection system.

The applicant's overpressure mitigation system is to be incorporated in two phases. The applicant has proposed an interim fix during the first fuel cycle and a final permanent fix at a later date. We require that the permanent fix be installed prior to startup following the first scheduled refueling shutdown. The interim fix is a combination of administrative procedures and operator training.

The following interim procedures are for plant operation below a system temperature of 250 degrees Fahrenheit during heatup and 260 degrees Fahrenheit during cooldown.

- (1) Whenever reactor coolant system pressure and temperature conditions permit, a pressurizer steam volume of at least 800 cubic feet will be maintained. The only situation expected when a steam bubble is desirable and cannot be maintained is during heatup when venting is being done prior to formation of a steam bubble. During the venting process operator procedures must require that an operator be assigned to monitor the reactor coolant system pressure.
- (2) Since the high pressure safety injection pumps are not required until a cold leg temperature of 200 degrees Fahrenheit is achieved, all high pressure safety injection pumps must be disabled below a system temperature of 200 degrees as required by the operating procedures. A caution tag is to be placed on the pump switches stating that operation of this component will result in system overpressurization. The requirement to disable all high

pressure safety injection pumps below 200 degrees Fahrenheit shall be removed when the permanent overpressure mitigation system is installed.

From 200 degrees Fahrenheit to 300 degrees Fahrenheit, only one high pressure safety injection pump is required. Therefore, operating procedures shall require only one high pressure safety injection pump to be in service while in the 200 degrees Fahrenheit to 300 degrees Fahrenheit temperature range. This requirement to permit only one pump to be in service shall be removed when the permanent overpressure protection system is installed.

- (3) Operating procedures shall require that reactor coolant pumps be disabled unless a steam volume of 800 cubic feet is drawn in the pressurizer.
- (4) Pressurizer heaters shall be disabled whenever they are not required.
- (5) The charging pumps will be disabled whenever they are not required. Operating procedures shall state that during water-solid operation, only one charging pump will be operable to monitor the water-solid condition and the charging pump low pressure relief valve shall be lined up for protection. This relief valve shall be set at 430 pounds per square inch gauge. The limitations on the charging pumps may be removed when the permanent overpressure mitigation system fix is installed.
- (6) System pressure during heatup will be limited by operating procedures to 375 pounds per square inch gauge until a reactor coolant system temperature of 250 degrees Fahrenheit is achieved. Thereafter, the pressure can be raised without concern for exceeding the pressure-temperature limits.
- (7) System pressure during cooldown will be limited by operating procedures to 300 pounds per square inch absolute when reactor coolant system temperature is below 260 degrees Fahrenheit.
- (8) All safety injection tank outlet lines are isolated and the isolation valve controls disabled during low pressure and temperature operation.

When maintaining a pressurizer steam volume of 800 cubic feet, the reactor coolant system is not vulnerable to inadvertent charging/letdown imbalance of any achievable magnitude. However, during the period of the interim fix, transients involving high pressure safety injection pumps remain a concern and item (2), above, will help minimize the potential for any such inadvertent pump injection. All other water-solid overpressure events considered are satisfactorily mitigated by the procedures above. In addition, an alarm is available when the shutdown cooling system is in operation to indicate reactor coolant system pressure exceeding 300 pounds per square inch absolute. Shutdown cooling suction valves 2CV-5084 and 2CV-5086 close automatically when the pressure reaches 300 pounds per

square inch absolute. When in the shutdown cooling mode, at least one low pressure safety injection pump will be running. If a low pressure safety injection LPSI pump is running and both shutdown cooling suction valves are not completely open, an alarm on the valves sounds in the control room.

The permanent fix for the water-solid overpressure protection system will consist of administrative procedures, alarms, and equipment modification. Two low setpoint relief valves, 2PSV-4732 and 2PSV-4742, and their isolation valves will be installed on the pressurizer. They will be lined up for use when the reactor coolant system temperature is reduced to 260 degrees Fahrenheit during cooldown. During heatup, the low setpoint relief valves will be isolated whenever the temperature is increased to 250 degrees Fahrenheit.

The design of the permanent fix requires only that the operator line up the low setpoint relief valves during cooldown and isolate during heatup to ensure low temperature water-solid overpressure protection.

The following criteria are applicable to the design.

- (1) No credit was taken for operator action after the low setpoint relief valves have been lined up. The relief capacity of one relief valve can accommodate a full safety injection actuation from a water-solid condition. Since the inadvertent safety injection transient is the worst-case event, all postulated transients are covered by this design.
- (2) The valving arrangement meets the single failure criteria.
- (3) The capability to test the relief valves has been incorporated into the system design. Testing will be done in accordance with the requirements of the ASME Code, Section XI.
- (4) The applicant has indicated that the relief valve design isolation valve control circuitry meets seismic Category I and IEEE Standard 279 criteria. This area is still under review by the staff and will be discussed in a future supplement. Similarly, the overpressure protection relief valves must be evaluated with respect to seismic criteria.

A revision to the Appendix G pressure-temperature limit curves has been submitted by the applicant to restrict the cooldown rate below 225 degrees Fahrenheit to 40 degrees Fahrenheit per hour. This change decreases the probability of a water-solid overpressure event. To assure operation of the overpressure mitigating system, the licensee is to submit, for staff review, a technical specification to implement this change. This specification is to be consistent with the intent of the statements listed below.

- (1) Unless both overpressure mitigation system trains are operable, reactor coolant system temperature may not be reduced below 275°F when the shutdown cooling system is in operation.
- (2) Operability of the overpressure mitigation system trains requires that the low temperature overpressure mitigation system isolation valves be capable of opening.

Conclusions

The staff has reviewed the proposed administrative changes for the interim fix and finds them acceptable as an interim measure to minimize the likelihood of a water-solid overpressurization event.

The potential effects of water-solid overpressurization for ANO-2 have been reviewed. Because of the minimal radiation damage suffered by the pressure vessel during its first operating cycle, we have concluded that even if an overpressure event resulted in system pressure reaching the safety valve setpoint value, sufficient margin to preclude vessel rupture still exists.

Because of the applicant's proposed interim administrative procedures and the pressure vessel fracture toughness, we have concluded that the reactor can operate for its first cycle with reasonable assurance that the health and safety of the public are protected.

The staff has reviewed the proposed permanent fix for low temperature water-solid overpressurization and finds it acceptable as a measure to minimize the likelihood of a water-solid overpressure event subject to completion of the two matters identified below. A condition to the operating license will stipulate that the permanent fix must be acceptably implemented by the applicant prior to startup following the first scheduled refueling shutdown.

- (1) The applicant must provide an interlock or alarm on the isolation valves which meets the applicable IEEE Standard 279 criteria and seismic Category I criteria for valves numbered 2CV-4730-1, 2CV-4731-2, 2CV-4720-2 and 2CV-4741-1, such that if the reactor coolant system temperature drops below the proposed temperature, and all the isolation valves are not fully open, an alarm sounds in the control room or the isolation valves open automatically.
- (2) The electrical portion of the permanent fix is still under review for conformance to safety-grade criteria.

With the resolution of the items noted herein, we conclude that the reactor can operate after installation of the permanent fix with reasonable assurance that the health and safety of the public are protected.

5.8 Loose Parts Monitoring

We addressed the ANO-2 loose parts monitoring system in Section 5.8 of the Safety Evaluation Report and stated that upon conclusion of our review we would report the results of that review in a supplement to the report.

We have completed our review of the loose parts monitoring system provided for ANO-2. The system is described in a letter dated August 31, 1977 from the applicant. The scope of the review was limited to a determination that a system is being provided and that the installed system will have monitoring capability comparable to that of systems employed on other operating reactors. The applicant has agreed to have the system installed and operational and to monitor the system for loose parts prior to initial criticality. Subject to documentation of this commitment, the staff finds the ANO-2 loose parts monitoring system to be acceptable. Any future requirements resulting from a present generic study being conducted by the staff on the implementation and utilization of such systems will be applicable to ANO-2.

7.0 INSTRUMENTATION AND CONTROLS

7.1 General

In the Safety Evaluation Report we identified items numbered 16 and 17 below that as a result of our site visit were unresolved and required additional documentation. Subsequent to the preparation of the Safety Evaluation Report we also determined that additional information was required on items numbered 5, 7, 10 and 15 below. In response, the applicant submitted additional information for our review. As a result of our review of the applicant's responses to the total list of 17 items identified in the site visit we conclude that the responses are acceptable except for the following items as identified in our letters to the applicant dated September 7, 1977 and November 29, 1977.

- (5) Installation of thermal barriers around cables.
- (7) Service water pumphouse sump level indication.
- (10) Protection of diesel generator controls.
- (15) Instrumentation connected to common sensing lines.
- (16) Redundant conduit separation.
- (17) Reinstatement of nonsafety loads on safety buses.

The applicant has responded to each of the above items. We will review this information and report our evaluation in a supplement to this report.

7.2 Reactor Trip System

7.2.2 Reactor Trip System - Hardwired Analog Portion

Independence of Redundant Power Supplies

In Section 7.2.2 of the Safety Evaluation Report, we identified concerns regarding the adequacy of independence provided in the design of the redundant plant protection systems and in the independence of the redundant vital buses. The design requires that the power supplies to the protection channels be valid isolation devices. The staff required information based on tests to demonstrate that a single failure in the circuits associated with the vital power supplies would not compromise the independence of the systems nor the independence of the redundant vital buses.

A test report, titled "Auctioneered Power Supply Type Test Report," was reviewed and the results were reported in the Safety Evaluation Report. In response to our evaluation of the above mentioned report, another report, titled "Input Fault and Surge Testing of Power Supplies," was submitted and reviewed. These tests included fault voltages of 140 volts direct current and 508 volts alternating current and surge tests in accordance with the recommendations established in IEEE Standard 472-1974.

The staff concludes that the information provided in this report is inconclusive and incomplete to support the design and the claim that the power supplies are valid isolation devices. The information does not adequately demonstrate that the effects of these faults and surges on the protection system are negligible, nor does it adequately address that the resulting perturbations on the output of these devices are acceptable. We therefore require the following:

- (1) That the response be amended and auditable test data results be provided with sufficient analysis, basis and justification to justify that the effects of the postulated fault and surge voltage transients do not degrade the safety channels and redundant vital buses below acceptable levels.
- (2) Information to demonstrate that adequate margin is provided in the design.
- (3) The design be modified to assure complete independence of redundant systems. The response should address, but not be limited to, spurious actuation of protection systems due to these surges and faults (if any), and the effects (if any) on the response times of these systems.

We will review the responses when submitted and report our evaluation in a supplement to this report.

7.2.3 Core Protection Calculator System Reactor Trip System-Digital Computer Portion

Introduction

Our Safety Evaluation Report included an introductory discussion on the core protection calculator system (CPCS).

The CPCS is designed to provide reactor protection for two conditions: (1) low local departure from nucleate boiling ratio (DNBR), and (2) high local power density (LPD). The remaining twelve of fourteen protective functions of the reactor protection system are accomplished by using a conventional analog hard-wired system. The detailed description and our evaluation and conclusions for the hard-wired portions of the protection system are presented in the Safety Evaluation Report and in Appendix D of this report.

This report contains review evaluation results established by the staff subsequent to the generation of the Safety Evaluation Report. Our evaluations are presented with respect to the safety positions defined in Table 7.1 of the Safety Evaluation Report, which for convenience are repeated as Table D.1 of this report. Section D.2 of this report is concerned with design basis, D.3 with the evaluation of protection algorithms, D.4 with hardware and software design and qualification, while Table D.3 presents references.

SUMMARY

Although the CPCS review is incomplete at this time, a majority of the information required to conduct the review has been docketed and evaluated. This information consists of detailed design documents for the stored computer programs and qualification test reports for both the hardware and software of the system. The evaluation of the acceptability of these documents as resolutions to the staff's safety position is presented herein. Based on the satisfactory resolution of staff concerns newly defined herein, and of the safety issues which are still outstanding, we see no reason at this time to conclude that the design and qualification of the system is unacceptable.

System Description

A description of the core protection calculator system may be found in Section 7.2.3 of the Safety Evaluation Report.

Staff Review Methodology

In addition to our comments regarding the staff's review methodology presented in the Safety Evaluation Report we note that in retrospect, the staff's review of the core protection calculator system has been conducted in two phases. The first review began in May of 1975, required several rounds of questions, meetings, and audits to obtain and evaluate information. The first phase of the review was terminated with the issuance of position 24 in September 1976. Position 24 contained the bases for rejection of the Phase II Test Report as qualification of the stored computer programs.

In response to position 24, and to the previous positions issued as of September 1976, the applicant committed to a redesign and a requalification effort for the stored computer programs. This effort consisted of the establishment of functional requirements, a design, a development, and a test of the stored computer program as depicted in Figure 7.1. The major documents reviewed by the staff for each portion of this effort are also shown in Figure 7.1. A safety evaluation of these reports is contained herein.

FIGURE 7.1 FUNCTIONS AND DOCUMENTS ASSOCIATED WITH
REDESIGN AND REQUALIFICATION OF STORED COMPUTER PROGRAMS

Functional Requirements	Design	Development	Test
CEN-44(A)-P CPC Functional Description and Supplement 1(P) Supplement 2(P) Supplement 3(P)	CEN-53(A)-P CPC/CEAC Data Base and Supplement 1(P) Supplement 2(P)	CEN-67(A)-P CPC/CEAC Program Assembly Listing	CEN-65(A)-P Phase I Test Audit CEN68(A)-P Phase II Test Audit
CEN-45(A)-P CEAC Functional Description	CEN-57(A)-P CPC Software Specification and Supplement 1(P) CEN-58(A)-P CEAC Software Specification CEN-55A Phase II Test Procedure and Supplement 1(P) CEN-69(A)-P CPC/CEAC Executive System Software Specification		CEN72(A)-P Phase I Test Report CEN73(A)-P Phase II Test Report CEN-60(A) Core Protection Calculator Integrated System Burn-In Test Procedure

The majority of the CPCS design and qualification information received from February 1977 to early January 1978 has been reviewed and is evaluated herein. Additional test information, in the form of test procedures and test reports are required from the applicant for staff review and evaluation. Also, information defined by the staff is required from the applicant to address outstanding questions. A review and evaluation of this information, test procedures, test results, and of technical specifications will be reported in a supplement to this report.

Details on the safety evaluation of the core protection calculator system are presented in Appendix D to this report.

CPCS Review Status Summary

The disposition of the 27 safety positions stated in Table D.1 are as follows:

- (1) The applicant has responded to and fully implemented to the staff's satisfaction 17 of the 27 safety positions generated by the staff. The issues designated as items 2, 3, 6, 7, and 17 in Table D.1 were resolved in the Safety Evaluation Report and are categorized as closed issues. The issues designated as items 8, 9, 10, 11, 13, 16, 21, 22, 23, 24, 25 and 27 in Table D.1 have been resolved to the staff's satisfaction as discussed herein and are now categorized as closed issues.
- (2) Ten of the safety positions defined in Table D.1 remain outstanding. These consist of positions 1, 4, 5, 12, 14, 15, 18, 19, 20 and 26. With respect to positions 1, 5 and 12, the applicant's responses to date have been reviewed and are acceptable. Start-up test data and analyses are required to evaluate the compliance with the remaining concerns. The applicant has committed to conduct the desired start-up tests and provide a test report to the staff. These positions are therefore resolved for the purpose of issuance of an operating license. Conditions to the operating license will require that these tests for which reactor operation is required be acceptably completed during the start-up phase of operations. A review and discussion of these positions are presented in the following sections of Appendix D to this report:

<u>Position</u>	<u>Section</u>
1	D.3.1
5	D.4.1.2
12	D.4.4.4

Positions 4, 14, 15, 18, 19, 20 and 26 remain outstanding. A review and discussion of these concerns are presented in the following sections of this report:

<u>Position</u>	<u>Section</u>
4	D.4.1.4
14	D.4.2.4
15	D.3.11
18	D.4.4.5
19	D.4.4.6
20	D.4.2.3
26	D.4.1.4

The staff will require that the foregoing matters be resolved with the applicant prior to plant start-up.

7.3 Engineered Safety Features Systems

7.3.2 Engineered Safety Features Actuation and Basic Logic

In Section 7.3.2 of the Safety Evaluation Report we stated in item (1) that either a high containment pressure or low pressurizer pressure signal would actuate the containment isolation system or the penetration room ventilation system. This is incorrect, as low pressurizer pressure does not actuate either of these two systems. Part (1) should have read:

(1) Containment isolation actuation system and penetration room ventilation system; high containment pressure.

Our conclusions with respect to our review of the engineered safety features systems remain as stated in the Safety Evaluation Report.

7.6 Other Systems Required for Safety

7.6.3 Safety-Related Fluid Systems

In Section 7.6.3 of the Safety Evaluation Report we stated that the requirements of Branch Technical Position EICSB No. 18, "Application of the Single Failure Criterion to Manually-Controlled Electrically-Operated Valves," had been implemented only in part in regard to the requirement for a second channel of position indication for valve 2CV-5628-2. The applicant was requested to modify the position indication design for this valve to provide redundant position indication in the control room that would meet the single failure criterion.

The applicant submitted a response to this item in letters dated October 7, 1977 and January 11, 1978, which we have reviewed and found to be unacceptable. Implicit in satisfying the single failure criterion, along with achieving independence, is that the equipment be capable of performing its intended function at all times, and therefore it must be qualified to the environmental and seismic

conditions of its location during all modes of plant operation. In a meeting between the staff and the applicant on January 26, 1978, the staff provided clarification of the above requirements by stating that the design of the second valve position indication channel must be designed to meet seismic Category I and IEEE Standard 279 requirements and criteria from the valve position sensor through to the indication components in the control room.

We therefore require the applicant to amend the response to this matter in accordance with the position stated above. We will review the information when submitted and report our evaluation in a supplement to this report.

7.6.4 Reactor Coolant Pump Coastdown Capabilities

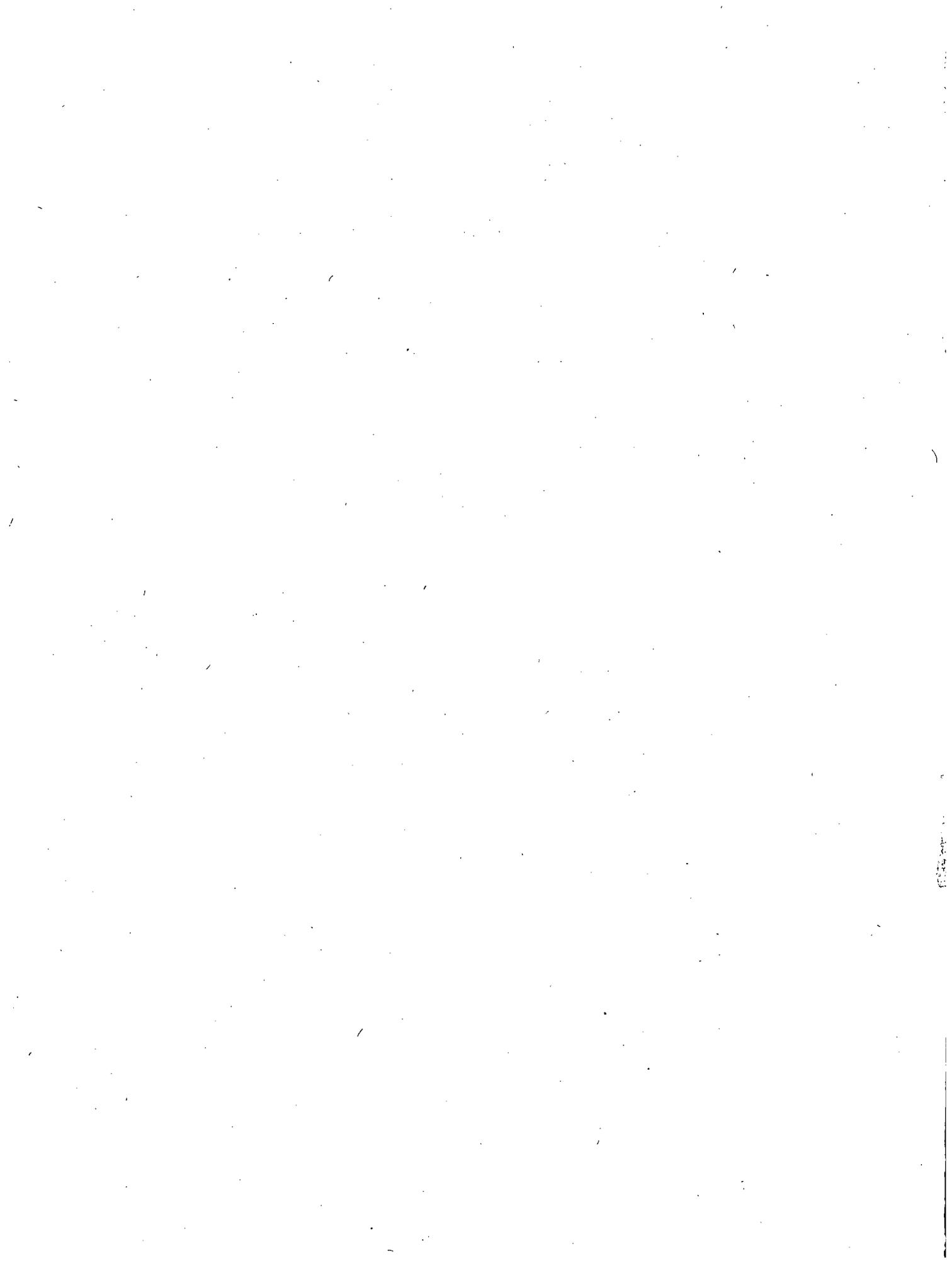
In Section 7.6.4 of our Safety Evaluation Report we stated that the applicant had submitted analyses to demonstrate that in the event the pump breakers failed to isolate the power supplies during an underfrequency condition, the reactor protection system would trip the reactor in sufficient time to preclude the reactor from going below the minimum departure from nucleate boiling ratio limits. We concluded that the analyses submitted demonstrated the design to be acceptable subject to the submittal and review of additional confirmatory analyses at power levels between the two power levels previously provided.

As stated in the Safety Evaluation Report, the applicant presented an analysis in Amendment 43 to the Final Safety Analysis Report for the results of a 6.47 Hertz per second grid decay rate at 30 percent power. Thirty percent power is the power at which the maximum decay rate of 6.47 Hertz per second occurs.

The analysis showed that the minimum departure from nucleate boiling ratio remained above 1.3. Likewise, the expected decay rate of 3.1 Hertz per second at 100 percent power is conservatively bounded by the loss of flow analysis included in Section 15.0 of the Final Safety Analysis Report.

Additional analyses at 6.47 Hertz per second and 50 percent power and at 3.88 Hertz per second and 80 percent power likewise demonstrate that the minimum departure from nucleate boiling ratio does not go below the 1.3 limit for these underfrequency events.

Therefore, we conclude that the applicant has demonstrated that adequate departure from nucleate boiling ratio protection exists at ANO-2 for credible grid decay events and that the design of the ANO-2 protection system is acceptable for protection against underfrequency or grid decay events in this regard.



14.0 INITIAL TESTS AND OPERATION

In Section 14.0 of the Safety Evaluation Report we discussed the performance of control element assembly drop time testing. We stated that our position with respect to the requirement to perform rod drop time testing at no flow conditions was that the omission of such tests would be acceptable to the staff only if the ANO-2 technical specifications prohibited rod withdrawal with fewer than two reactor coolant pumps in operation.

Subsequently, in Amendment No. 44 to the Final Safety Analysis Report, the applicant added testing at the cold shutdown conditions with no reactor coolant flow. This testing is acceptable to meet our requirements for testing at the no flow condition. However, in Amendment No. 44 the applicant deleted the commitment to perform rod drop tests at hot shutdown conditions with two or three reactor coolant pumps in operation.

We have informed the applicant that we will require the reinstatement of testing at hot shutdown conditions. The applicant has agreed to reinstate these tests and, therefore, this matter is resolved pending the documentation in the Final Safety Analysis Report of the commitment to perform rod drop time testing for the hot shutdown partial flow, cold shutdown no flow, and hot zero power full flow conditions.



15.0 ACCIDENT ANALYSIS

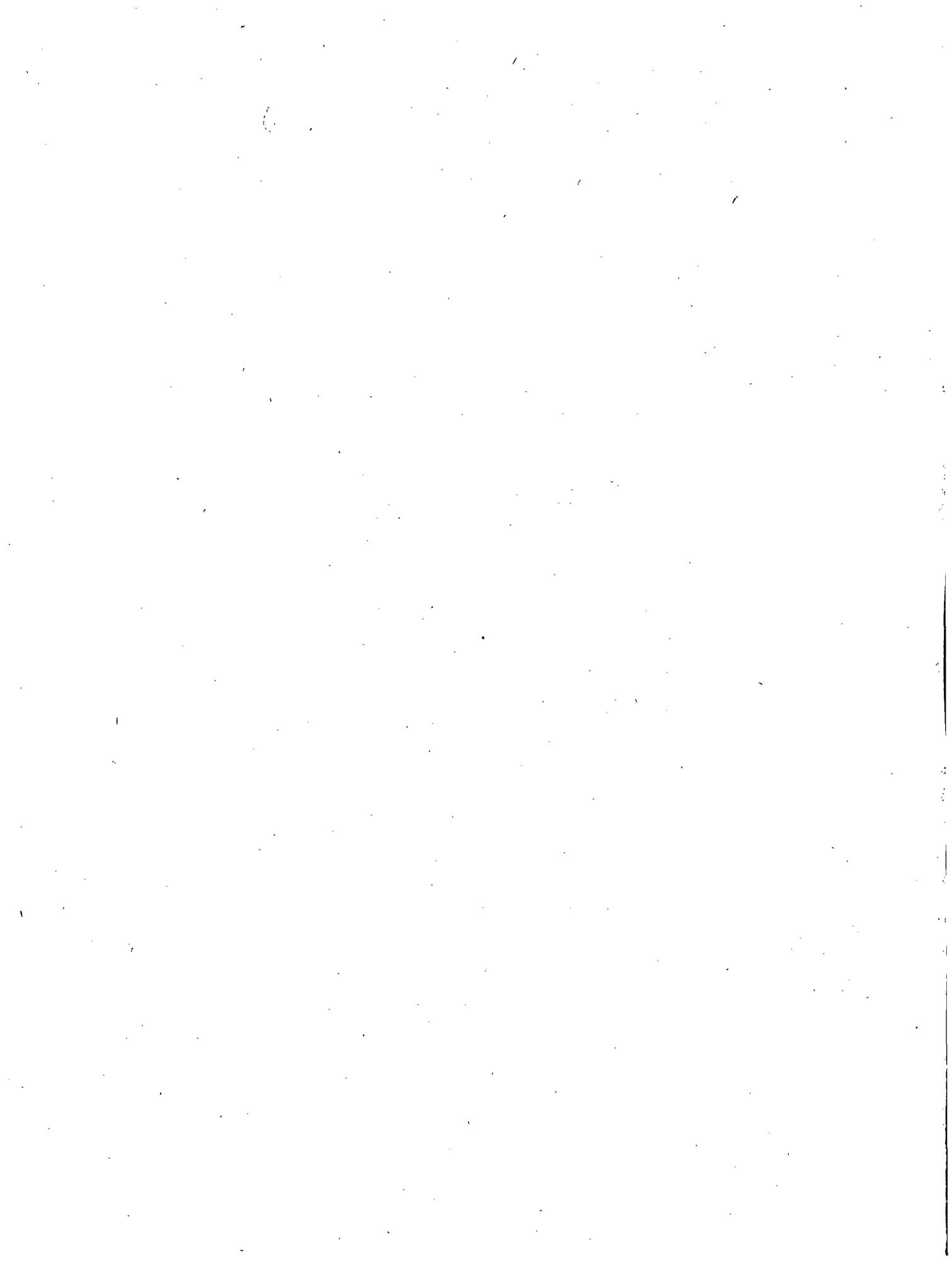
15.4 Postulated Accidents

15.4.7 Fuel Handling Accident

In Section 15.4.7 of the Safety Evaluation Report we reported our evaluation of a postulated fuel handling accident in the spent fuel pool area of the auxiliary building but stated that we had not completed our evaluation of a postulated fuel handling accident within the containment.

The applicant has described the protective measures to provide assurance that a refueling accident within containment would not result in significant releases of activity to the environs. These measures consist of the following: (1) during refueling operations, all pathways providing direct access to the outside atmosphere will be closed except for the containment purge valves, and (2) purge exhaust during refueling operations will be conducted through containment purge filter units which are identical in design to the filter units in the fuel handling area ventilation system described in Table 9.4-3 of the Final Safety Analysis Report. We conclude that the radiological consequences of this accident are bounded by the radiological consequences of a fuel handling accident in the spent fuel pool area and are therefore acceptable.

Based on the above commitments by the applicant, which are also included in the technical specifications, we conclude that adequate measures have been provided to assure that significant quantities of radioactive materials will not be released as a result of a postulated refueling accident within the containment.



APPENDIX A

SUPPLEMENT TO THE CHRONOLOGY OF THE
RADIOLOGICAL SAFETY REVIEW

October 7, 1977	Applicant letter transmitting responses to staff's letter of September 7, 1977.
October 13, 1977	Applicant letter transmitting additional proposed technical specifications.
October 21, 1977	Staff letter transmitting list of deficiencies found in the amended security plan.
October 25, 1977	Staff letter on physical security assessment models subject to the requirements of 10 CFR 73.55(a).
October 25, 1977	Applicant letter transmitting additional proposed technical specifications.
October 26, 1977	Applicant letter transmitting answers to staff questions on fire protection.
November 3, 1977	Staff letter stating position on reactor vessel support system analyses.
November 4, 1977	Applicant letter transmitting information on emergency cooling pond.
November 11, 1977	Staff letter requesting information on containment leakage testing program.
November 11, 1977	Staff letter requesting information on diesel generator lockout.
November 14, 1977	Staff letter concerning Section 6.0 of the Technical Specifications.
November 17, 1977	Applicant letter requesting an extension of the latest dates for completion of construction.

November 17, 1977	Staff letter requesting additional information on fire protection
November 18, 1977	Staff letter requesting additional reactor systems information.
November 23, 1977	Staff letter on the CESEC Code verification testing program.
November 23, 1977	Staff letter requesting information on pressure vessel fracture toughness.
November 28, 1977	Staff letter on amendment to 10 CFR 73.55.
November 29, 1977	Staff letter requesting information on July 6, 1978 site visit items.
December 1, 1977	Staff letter providing guidance on conformance to 10 CFR 50.55a(g).
December 5, 1977	Staff letter on the Emergency Plan.
December 5, 1977	Staff letter on fracture toughness and potential for lamellar tearing of steam generator and reactor coolant pump support materials.
December 6, 1977	Applicant letter (unsigned) regarding the schedule for provision of fire protection information.
December 7, 1977	Applicant letter transmitting responses to reactor systems questions of staff's November 18, 1977 letter.
December 9, 1977	Staff letter on core protection calculator system preoperational testing.
December 12, 1977	Applicant letter transmitting modifications to the software burn-in test procedure.
December 19, 1977	Applicant letter transmitting additional proposed technical specifications.
December 20, 1977	Applicant letter transmitting information on the ANO-1 and ANO-2 fire hazards analysis.
December 20, 1977	Amendment No. 44 submitted.

December 22, 1977 Staff letter requesting information on fuel assembly burnable poison rods and control element assembly absorber material.

December 27, 1977 Staff letter on instrumentation and control system logic.

December 30, 1977 Applicant letter transmitting responses to staff's letter of November 11, 1977 on diesel generator lockout.

January 4, 1978 Applicant letter responding to staff letter of August 4, 1977 on MSLB Environmental Qualifications.

January 6, 1978 Applicant letter advising that response to staff letter of December 5, 1977 on the Emergency Plan would be provided by February 28, 1978.

January 6, 1978 Applicant letter transmitting additional proposed technical specifications.

January 10, 1978 Applicant letter transmitting information on CPCS Position 24.

January 11, 1978 Applicant letter transmitting responses to staff's September 7, 1977 letter on sump testing, seismic qualifications, and valve position indication.

January 16, 1978 Applicant letter responding to staff's letter of November 29, 1977 on the I&CSB site visit items.

January 17, 1978 Applicant letter providing information on increase in local pin power peaking.

January 17, 1978 Applicant letter transmitting responses to staff's letter of June 18, 1976 on reactor vessel supports.

January 18, 1978 Applicant letter advising that Agastat Timer Environmental Qualification information will be delayed.

January 18, 1978 Staff letter requesting additional information in seven areas of the core protection calculator system review.

January 18, 1978 Applicant letter transmitting CEN-74, Isolation Test Report.

January 19, 1978 Applicant letter transmitting partial response to staff's letter of November 11, 1977 on containment leakage testing.

January 20, 1978 Applicant letter transmitting response to staff's letter of September 7, 1977 on GE relay seismic qualification.

January 20, 1978 Applicant letter transmitting response to staff's letter of September 7, 1977 on seismic qualification of core protection calculator system components.

January 24, 1978 Applicant letter transmitting response to staff's letter of February 3, 1977 on offsite power systems.

January 25, 1977 Applicant letter transmitting information on the vibration testing of reactor coolant piping.

January 26, 1978 Staff letter transmitting evaluation of CEN-74, Isolation Test Report, to applicant.

January 26, 1978 Meeting between staff and applicant to discuss completion of licensing activities.

January 27, 1978 Applicant letter transmitting response to staff's letter of September 7, 1977 on the steam line break accident analysis.

January 31, 1978 Applicant letter transmitting response to staff's letter of August 24, 1977 on main steam line break mass and energy release.

February 2, 1978 Advisory Committee on Reactor Safeguards Subcommittee meeting in Washington, DC on safety matters outside of the core protection calculator system review.

February 3, 1978 Applicant letter transmitting information on the fire hazards analysis.

February 6, 1978 Staff letter (undated) providing procedure and acceptance criteria for the development of the inservice testing of pumps and valves.

February 9, 1978 Advisory Committee on Reactor Safeguards meeting in Washington, DC on safety matters outside of the core protection calculator system review.

Supplement No. 1 to
APPENDIX B

Bibliography for
Arkansas Nuclear One-Unit 2
Safety Evaluation Report

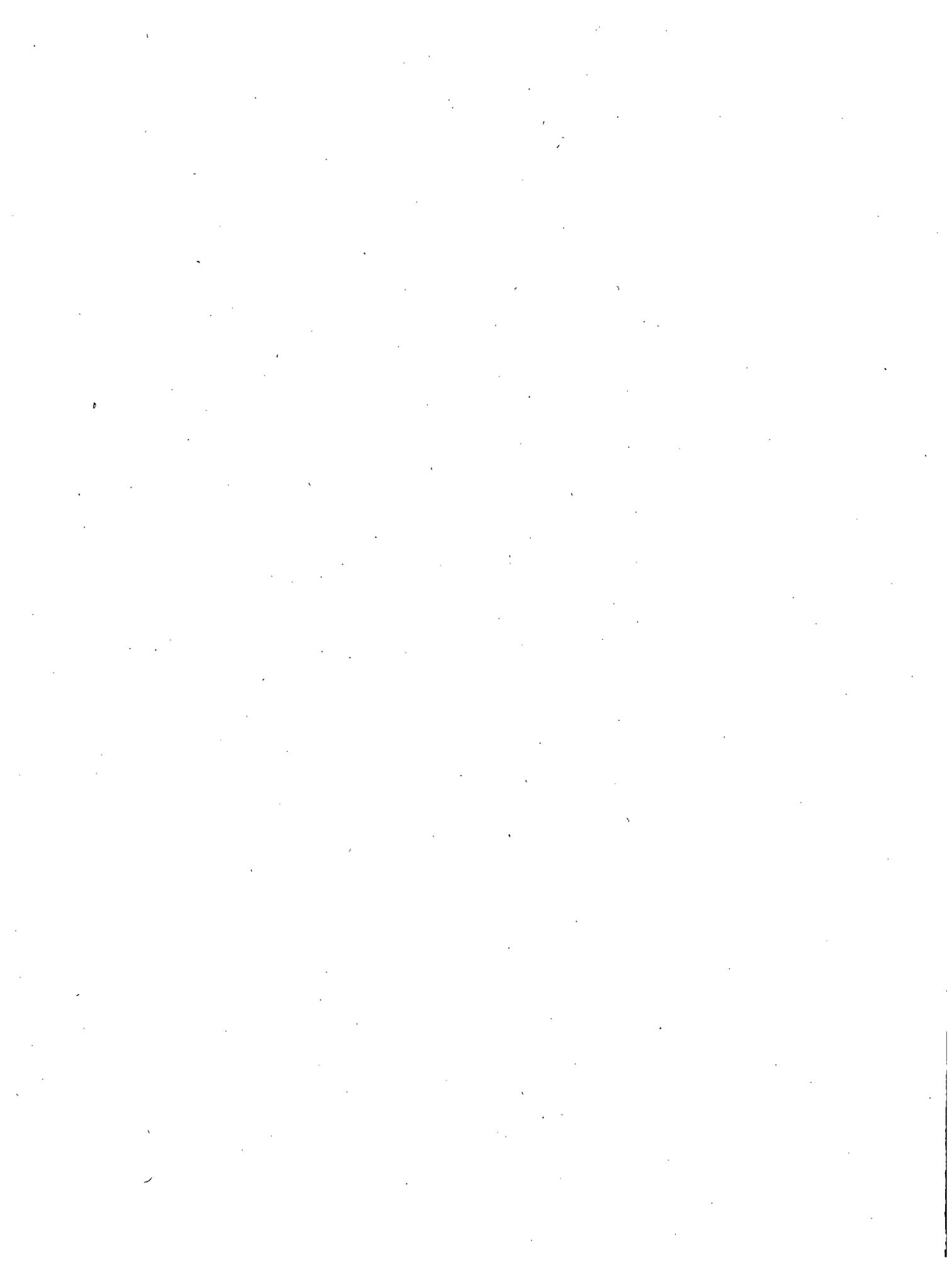
NOTE: Documents referenced in or used to prepare this Safety Evaluation Report may be obtained at the source stated in the bibliography or, where no specific source is given, at most major public libraries. Correspondence between the Commission and the applicant (Final Safety Analysis Report, Environmental Report, and application) and Commission Rules and Regulations and Regulatory Guides may be inspected at the Commission's Public Document Room, 1717 H Street, N.W., Washington, DC. Correspondence between the Commission and the applicant may also be inspected at the Arkansas Polytechnic College Library, Russellville, Arkansas. Specific documents relied upon by the Commission's staff and referenced in this Safety Evaluation Report are listed as follows:

Geography and Demography

1. Manes and Associates, "The Planning Document, Russellville, Arkansas," April 1976. Available in NRC Public Document Room as an attachment to applicant's letter dated September 27, 1977.
2. Manes and Associates, "Zoning Ordinance, Russellville, Arkansas, "August 10, 1976. Available in NRC Public Document Room as an attachment to applicant's letter dated September 27, 1977.

Reactor

3. NRC memorandum, D. F. Ross and D. G. Eisenhut to D. B. Vassallo and K. R. Goller, "Revised Interim Safety Evaluation Report on the Effects of Fuel Rod Bowing on Thermal Margin Calculations for Light Water Reactors," dated February 16, 1977. Available in the NRC Public Document Room.



Appendix D

TABLE OF CONTENTS

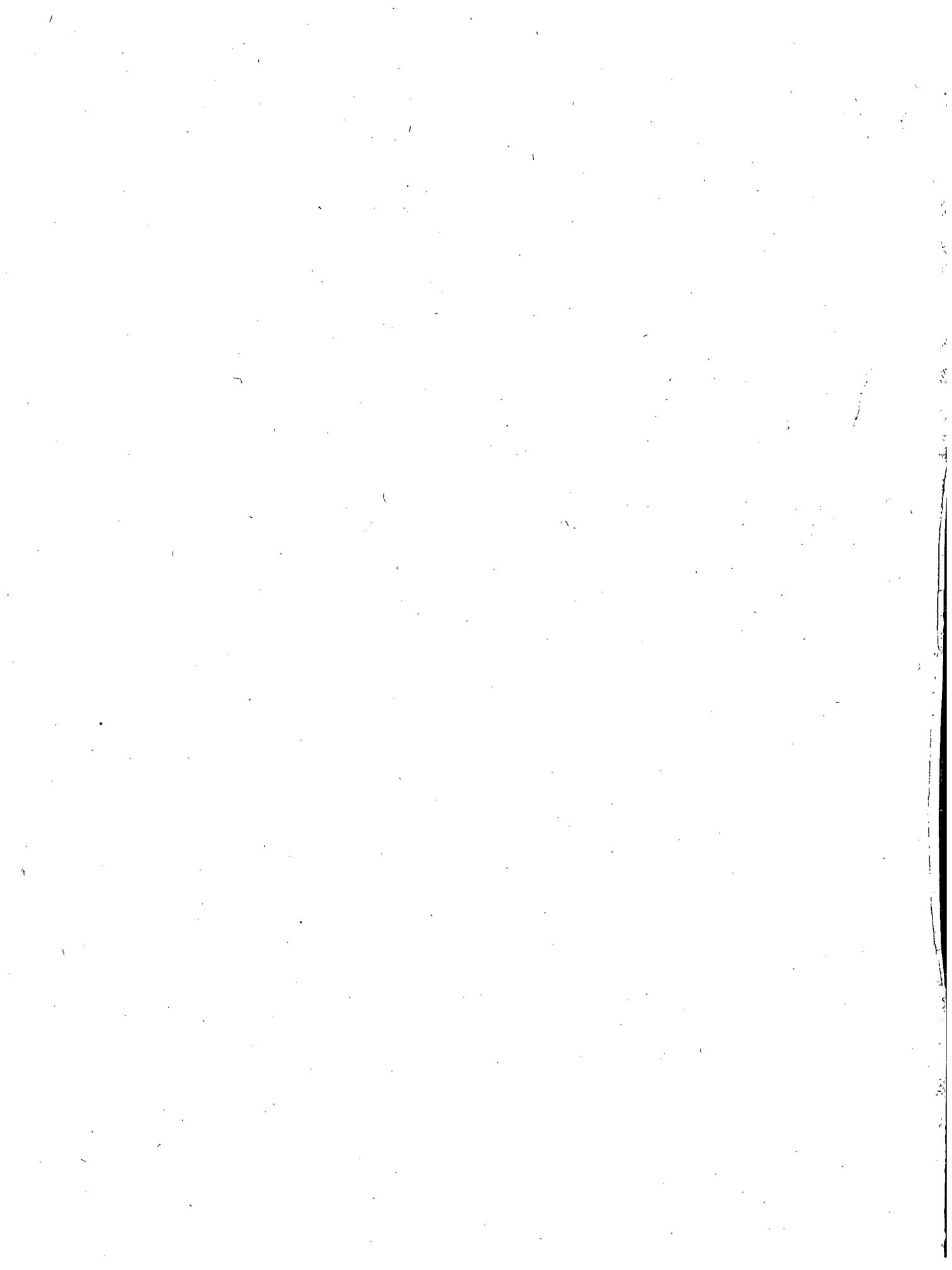
	<u>PAGE</u>
D.1 General.....	D-1
D.2 Design Basis.....	D-1
D.3 Protection Algorithms.....	D-3
D.3.1 Axial Power Distribution Synthesis.....	D-3
D.3.2 Radial Power Distribution Synthesis.....	D-3
D.3.5 Power Distribution Uncertainty.....	D-3
D.3.6 Uncertainty Assessment.....	D-4
D.3.7 Primary Coolant Mass Flow Algorithm.....	D-4
D.3.8 Minimum DNBR Algorithm.....	D-5
D.3.9 Core Thermal Power Algorithm.....	D-7
D.3.11 Addressable Constants.....	D-8
D.4 Design and Qualification.....	D-9
D.4.1 Hardware Design.....	D-9
D.4.1.2 Signal Generation and Process Equipment for the CPCS.....	D-9
D.4.1.3 Core Protection Calculator.....	D-10
D.4.1.4 Control Element Assembly Calculator (CEAC).....	D-11
D.4.1.6 Bypasses and Interlocks.....	D-13
D.4.2 Test, Maintenance, Monitoring and Qualification.....	D-14
D.4.2.1 Operational Testing.....	D-14
D.4.2.2 Maintainability.....	D-17
D.4.2.3 Plant Computer System Monitoring.....	D-18
D.4.2.4 Environmental Qualification.....	D-20
D.4.2.5 Seismic Qualification.....	D-21
D.4.2.6 Pre-Operational Test.....	D-21
D.4.3 Software Design Evaluation.....	D-22
D.4.3.1 General.....	D-22
D.4.3.2 Documentation.....	D-23
D.4.3.3 Quality Assurance.....	D-24

TABLE OF CONTENTS (Continued)

	<u>PAGE</u>
D.4.4 Software Qualification.....	D-25
D.4.4.1 Phase I Test Plan.....	D-25
D.4.4.2 Phase I Test Results.....	D-26
D.4.4.3 Phase II Test Plan.....	D-28
D.4.4.4 Phase II Test Results.....	D-29
D.4.4.5 Integrated System Burn-In Test.....	D-32
D.4.4.6 Qualification of the Single Channel Test System for Testing of Future Software Modifications.....	D-34
D.4.4.7 Startup Tests.....	D-37

LIST OF TABLES

	<u>PAGE</u>
TABLE D.1 - CPCS POSITIONS.....	D-38
TABLE D.2 - CPCS REFERENCES AND MEETING MINUTES.....	D-51



Supplement No. 1 To
APPENDIX D

Core Protection Calculator System

D.1 General

This Supplement No. 1 to Appendix D of the Safety Evaluation Report presents further details of the staff's review evaluation results which have been established subsequent to the preparation of the Safety Evaluation Report. Section D.2 of this report is concerned with design basis, D.3 with the evaluation of protection algorithms, D.4 with hardware design and qualification, D.5 with software design and qualification while D.6 presents references.

Acronyms are extensively employed in certain sections of this appendix. Therefore, a listing of the most frequently used acronyms and their meaning is included below.

CPCS - core protection calculator system.
CPC - core protection calculator.
CEA - control element assembly, i.e., control rod.
CEAC - control element assembly calculator.
RSPT - reed switch position transmitter.
AC - alternating current.
DNBR - departure from nucleate boiling ratio.
LPD - local power density
COLSS - core operating limit supervisory system.
MACS - multipurpose acquisition control system.
I/O - input/output device.
PUPS - Power Utility Plant Simulator.

D.2 Design Basis

Because the core protection calculator system (CPCS) is a first of a kind design, the staff considered failure of the CPCS to perform its normal function. Backup trips and normal shutdown mechanisms were reviewed to assess the depth of protection provided. This extent of this review is beyond that normally performed for reactor protection systems.

The CPCS provides the initial, but not the only trip, for steam line break accidents, reactor coolant pump shaft seizure and steam generator tube rupture. Increased fuel damage could occur for the above accidents with concurrent failure of

the CPCS. However, analog backup trips on system pressure and pressurizer level are available to provide reactor shutdown and mitigate the consequences of accidents. Failure of the CPCS, concurrent with any of the above incidents is an extremely unlikely event.

The CPCS is designed to initiate a reactor trip for the following events:

- (1) Uncontrolled control element assembly (CEA) withdrawal from a critical condition.
- (2) CEA misoperation.
- (3) Uncontrolled boron dilution.
- (4) Total and partial loss of reactor coolant forced flow.
- (5) Excess heat removal due to secondary system malfunction.
- (6) Steam generator tube rupture with and without a concurrent loss of offsite alternating current (AC) power.

Backup trips are available to limit the consequences of each of the above events, even with failure of the CPCS, except for the CEA misoperation event.

The CPCS provides a reactor trip for CEA deviation events where DNBR or peak linear heat rate limits are approached. Automatic reactor trips have not been provided in previous Combustion Engineering protection system designs for this event. In the unlikely event that a CEA deviation event which required a reactor trip occurred without a CPC initiated trip, the operator would get alarms from the core operating limit supervisory system (COLSS) on CEA position and flux tilt similar to that in non-CPCS plants. Manual trip could then be initiated.

For the other events the applicant has stated that the backup trips are:

- (1) CEA withdrawal - high pressurizer pressure.
- (2) Boron dilution - high pressurizer pressure.
- (3) Total or partial loss of flow - high pressurizer pressure, low steam generator pressure, low steam generator water level. These trips also are available for loss of flow due to pump shaft seizure.
- (4) Excess heat removal - low steam generator water level, high pressurizer pressure, and low steam generator pressure.
- (5) Steam generator tube rupture - low pressurizer pressure.

The staff has considered failure of the digital trip system to perform its design function. Backup analog trips and/or inherent shutdown mechanisms limit the consequences of this type of failure for all but the CEA misoperation event. For CEA

misoperation, a manual trip, similar to previous plants, is required but numerous alarms and indications are available to inform the operator of the event. We find the backup to the CPCS to be acceptable.

D.3 Protection Algorithms

An initial review of the protection algorithms is reported in our Safety Evaluation Report. Subsequent to the initial review, the applicant conducted a redesign of the protection algorithms which instituted several modifications. The staff's evaluation of the redesign and modifications is reported herein.

D.3.1 Axial Power Distribution Synthesis

D.3.2 Radial Power Distribution Synthesis

D.3.5 Power Distribution Uncertainty

The review of the power distribution algorithms employed by the CPCS to determine the core average axial power shape, the three-dimensional form factor (F_Q), the pseudo-hot channel power distribution, and the axial shape index has been completed. Additional information submitted in references 3, 4, 5 and 6 and reviewed subsequent to the issuance of the Safety Evaluation Report supports the finding that the protection algorithms will conservatively predict the power distribution parameters used in the CPC calculation of the local power density (LPD) and departure from nucleate boiling ratio (DNBR) margins to the trip setpoints.

The calculation of the power distribution synthesis uncertainty to assure the appropriate conservatism has been updated. A more accurate calculational model of the ANO-2 reactor, in addition to an improved method for calculating the shape annealing matrix components, has led to a reduction of the synthesis uncertainty factor to 1.07. A review of the startup test requirements in reference 6 indicates that the startup tests will be adequate to experimentally verify this value of the uncertainty. Should a discrepancy exist between the measured and calculated values, contingencies have been presented in reference 5 for incorporating the differences into the CPC algorithms. Thus, at this stage of the licensing schedule, intent of Position 1 has been satisfied. The staff is also in the process of reviewing startup test procedures and we will report on our evaluation in a supplement to this report.

During the Phase II Test Audit discussed in reference 18, the staff observed that the continuous display of the penalty factor is not required. The penalty factor is derived from misalignments among the control element assemblies and is used as a modifier of radial peaking factor. Each core protection calculator is designed to select the maximum penalty factor upon comparing the penalty factor transmitted by each control element assembly calculator. Thus, a conservative value of the penalty factor is used in the low protection calculators. Continuous display of the penalty factor would merely serve to display non-essential information.

The review of the COLSS and INCA monitoring systems has been completed to a point where the staff finds the methodology acceptable. The final approval of the specific uncertainties associated with the ANO-2 implementation of these systems is continuing with a final resolution determined by the results of startup testing.

D.3.6 Uncertainty Assessment

The Topical Report CENPD-170, reference 9, describes the methods used in the CPCS to synthesize the three-dimensional peaking factor (F_Q). The resulting F_Q is used in conjunction with other measured parameters to determine a minimum DNBR. CENPD-170, Supplement 1-P, reference 10, provides additional discussion of the uncertainties associated with the synthesis of the minimum DNBR. The review of CENPD-170 and its supplement is presented in the Safety Evaluation Report. The methodologies used for thermal-hydraulic protection algorithms, including the evaluation of uncertainties, are acceptable to the staff.

Subsequent to the above described review, the applicant initiated a redesign and a requalification of the protection algorithms and the computer program. The staff conducted a reassessment of the protection algorithms in reference 3, of the uncertainties used in the algorithms, and of the data base required for the protection algorithms. The reassessment of these subjects included an audit, which is reported in reference M16.

We also audited the methodology and the values employed in establishing the uncertainties for the DNBR algorithm. This effort concentrated upon the uncertainties used in the formulation of the static DNBR algorithm. We found that the methodology employed and the values employed in the uncertainty assessment were satisfactory. The applicant was requested to docket the audited uncertainty calculation as an example of methodology used. The applicant has conformed to this request.

The protection algorithms in the core protection calculators evaluate thermal-hydraulic conditions in the hot channel using a snapshot of both directly monitored and calculated variables. The Combustion Engineering standard design code for computing DNBR is COSMO, an open hot channel thermal margin code. The CPCS uses a simplified closed channel fast running version of COSMO. The CPCS version has been derived from and justified with respect to the design code COSMO. COSMO has been approved for use in licensing applications.

The analytical tools and procedures used for synthesis of the static DNBR have been reviewed by the staff and found acceptable.

D.3.7 Primary Coolant Mass Flow Algorithm

The primary coolant mass flow algorithm computes a normalized flow rate in the reactor core. To compensate for computer execution delays and system lags, it also

computes a projected value of DNBR based on the time derivative of core flow rate. The normalized mass flow rates are computed from the speeds of the four reactor coolant pumps and the specific volume of the primary coolant.

The flow algorithm contains a representation of the flow resistance and flow inertia for each flow path in the reactor coolant system. The performance of each pump is represented by a steady-state set of head-flow-speed curves. The algorithm solves simultaneous differential equations expressing conservation of momentum and mass around closed flow loops through each pump to obtain core mass flow rate. Furthermore, it also selects pump-dependent uncertainty factors to be applied to the minimum DNBR and peak local power density evaluations.

As currently configured, the implemented data base for the mass flow protection algorithm is designed for four reactor coolant pump operation. Although the capability exists for part loop operation, the required data base constants have not been generated, implemented and qualified. To assure protection in the event of loss of one or more pumps, (indicated by decrease in pump shaft-speed) the staff required that a 40 percent power penalty be applied to the CPC calculated DNBR and LPD for part loop operation. This will assure reactor trip for loss of one or more pumps at high reactor power, yet allow for an orderly manual plant shutdown at low reactor power. Furthermore, a technical specification will prohibit deliberate operation with less than four primary coolant pumps in operation.

With reverse flow through an idle loop, the flow weighted thermal power calculation, with no compensation, will give a nonconservative value for the thermal power. However, the nonconservatism can be determined in advance and can be offset by a penalty factor applied through pump-dependent constants. These CPC constants have not been qualified for part loop operation for ANO-2, cycle 1, and thus, inadvertent part loop operation will be penalized as described above.

The forward flow coefficients for the mass flow algorithm will be verified during startup testing. If required from analysis of startup test results, modifications to the flow coefficients in the data base will be made and the program requalified for the modifications.

Based on the limitations stipulated above, the staff finds the design and proposed startup verification techniques for the mass flow algorithm acceptable.

D.3.8 Minimum DNBR Algorithms

The static departure from nucleate boiling ratio (DNBR) and power density program computes the static value of DNBR, hot channel quality, primary thermal power, and maximum hot leg enthalpy. The static DNBR program establishes the baseline conditions for the DNBR update.

Dynamic update of thermal margin limits is based on derivations of thermal-hydraulic variables, power distribution variables and core power variables from reference conditions computed in the static DNBR and power density algorithm. The update factors, which are partial derivatives of power with respect to each monitored and calculated state variable and of the partial derivative of DNBR with respect to power, were determined from the COSMO code thermal margin calculations over specified ranges of the monitored and calculated state variables. The partial derivative factors are dependent on the nature of the changes in the state variables. Further information on the partial derivative factors is contained in CEN-44(A)-P, reference three. The effects of changes in state variables are converted to equivalent overpower margin units by use of the partials and the results are then converted to DNBR and quality units. The change in DNBR is added to the current static DNBR and input directly in the CPC trip decision logic for comparison to the 1.3 safety limit. In addition, updated DNBR is compared to a modified DNBR operating limit value and the appropriate valve is selected for input to the CPCS mass flow rate projection logic, which provides protection against loss of flow events.

The CPC mass flow rate projection algorithm evaluates the time rate of change of mass flow based on the current and previously computed value of flow. The mass flow derivative is then multiplied by an appropriate partial derivative of DNBR with respect to flow rate times the projection time constant. The resulting DNBR for the projected flow rate is added to the modified DNBR operating limit or to the CPC current calculated value, whichever is greater. This yields the flow projected DNBR which is input to the CPC trip program for comparison to the 1.3 safety limit. The description of the method to calculate the flow projected DNBR is included in the Combustion Engineering topical report CEN-44 (A), reference three.

The DNBR updated algorithm is capable of predicting thermal margin changes caused by changes in the axial and radial power distribution. Changes in axial power distribution caused by rod movements are slow relative to the combined effect of the heat flux time constant and the cycle time of the static DNBR calculation. The CEA deviation penalty factor provides multipliers on the hot pin integrated radial peaking factor that includes the effects of axial power distribution changes in their values. Therefore, it was concluded that the update on the hot pin integrated radial peaking factor is sufficient for predicting margin changes due to axial power shape changes. The coefficient for the update on axial changes was set equal to zero in the current data base as described in references 5 and 12.

The functional description of the protection algorithms as described in reference 3 gives quality limits in the static DNBR algorithm which were to correspond to 20 and 60 percent void fraction limits. These void fraction limits have traditionally been used by Combustion Engineering as hydraulic stability limits. The applicant has justified in reference 42 that these limits are not needed to protect against hydraulic instabilities. The void fraction limits have been modified in the ANO-2 data base to provide protection against numerical instabilities. The staff finds this modification acceptable.

The CPC program calculates a third value of DNBR based on a projected depressurization transient at a rate determined from monitored values of pressure. However, in the initial CPC data base for ANO-2, this projected change in DNBR is nulled through the use of zero coefficients and is replaced with an offset in the overall power uncertainty term. This technique is acceptable. The pressure projection algorithm remains untested; therefore, approval of the CPCS does not constitute approval of the pressure projection algorithm.

Thus, two values of DNBR are calculated for comparison to the safety limit:

- (1) The static or updated DNBR based on the most recent scan of monitored state variables, and
- (2) The projected value of DNBR based on the change in the flow rate.

A DNBR value of 1.3 or less for either of the above will result in a DNBR trip signal. With the exception of the pressure projection algorithm (as described on page 68 of reference three and which is not used for ANO-2), we find the method of calculating minimum DNBR to be acceptable.

D.3.9 Core Thermal Power Algorithm

An evaluation of core thermal power and of neutron flux power is made for use in the protection algorithms. For conservatism, an auction of the highest value of power is made and then used in evaluating DNBR and local power density (LPD). Neutron flux power algorithms are discussed in the Safety Evaluation Report. The following discussion of core thermal power reflects our review of this subject subsequent to the Safety Evaluation Report.

The primary coolant system consists of two steam generator loops, with each of the loops having one hot leg and two cold legs for coolant transport. Reactor inlet temperature is measured in one cold leg of each steam generator loop for each CPC channel; also, each hot leg coolant temperature is monitored for each CPC channel.

The core thermal power is calculated in two components: a calculation of static power and a calculation of dynamic power. The static power calculation uses a flow weighted average of the enthalpy rise in each steam generator loop. For four-pump operation this method accounts for imbalances between steam generators and is an acceptable method for calculating the static core thermal power. For part loop operation, the staff has assessed that the methodology is nonconservative in the evaluation of static core thermal power. A justification of the core thermal power algorithm is one of several requirements for qualification of part loop operation.

The flow weighted power calculation is multiplied by a thermal power constant to obtain the reactor power. The value of the constant is selected for each CPC to

make the computed power equal to the power periodically determined by the plant secondary calorimetric calculation which is also checked with other available power level indicators.

The dynamic power calculation adds a correction term to the static power calculation to account for delays due to fluid transport times between sensors and the core, plenum mixing time and temperature sensor time constants. In the execution of the protection algorithms the highest value of core thermal power versus neutron flux power is selected. The determination of neutron flux power is discussed in the Safety Evaluation Report.

The staff has reviewed the methods of calculating and calibrating core thermal power. We find the methods acceptable for four-pump operation subject to the limitations stipulated in Section D.3.7. The current computer program is not qualified for operation unless all primary coolant pumps are in service.

D.3.11 Addressable Constants

To allow for reed switch position transmitter (RSPT) and/or control element assembly calculator (CEAC) failure, the CEAC/RSPT Inoperable (INOP) mode (CEAC Operating Bypass) has been implemented. The reactor operator activates the CEAC/RSPT INOP mode by a keyboard entry at the Operators Module. The keyboard entry in turn sets a flag in the stored computer program. The operation and implementation of the CEAC/RSPT INOP is described in section D.4.1.6. The functional impact upon reactor operation is discussed below.

When the INOP flag is set, the CPC program automatically sets the values of each CEA position, which it normally needs from the RPST sensors, at the value of its long-term insertion limit (LTIL). The LTIL for each control element assembly (CEA) are stored as constants in each CPC's protected memory. Also, the penalty factor read from each CEAC is ignored by the CPC for reactor operation in this mode. The technical specifications require that control rods be administratively monitored by the operator to a range of insertion varying from full-out to a maximum insertion equal to the LTIL. When the rods are within the range of full-out to the LTIL, the radial peaking factors applied to each mode down to the LTIL value add an element of conservatism to the CPC calculated power distribution. However, the rod shadowing factors applied in the protection algorithms for the INOP mode of operation may lead to a non-conservatism in the power calculation. To accommodate this effect, a penalty factor is automatically applied to the power calculation for the INOP mode of operation. This penalty factor, in addition to the conservative radial peaking factors, assures a conservatively high calculation of power parameters in the CEAC/RSPT INOP mode. We have reviewed these penalty factors and have found them to be acceptable.

With respect to the reasonability checks on addressable constants (position 15), all addressable constants have acceptable automatic range limit checks with the exception of the shape annealing matrix (SAM) components. The staff required reasonability checks of addressable constants as a method for detecting gross errors upon operator entry of an addressable constant. Conceptually, the reasonability checks are the equivalent of the limits of an adjustable potentiometer in conventional analog hard-wired type of protection systems.

The staff has requested that the applicant identify acceptable range limits on the shape annealing matrix components based on ANO-2 design calculation as stated in reference two. Thus, position 15 remains outstanding and we will address the resolution of this item in a supplement to this report.

D.4 Design and Qualification

D.4.1 Hardware Design

D.4.1.2 Signal Generation and Process Equipment for the CPCS

Process Instrumentation

Our review of the process instrumentation for the CPCS is presented in the Safety Evaluation Report. The review revealed that all of the analog sensor signal processing for the entire reactor protection system (RPS) is being processed and housed within the Process Protection Cabinet 2C15. This cabinet is 16 feet long and 10 feet high and is physically separated into four redundant channels. During the drawing review an associated circuit problem was identified within the 2C15 cabinet. The concern expressed by the staff was the close proximity of the Class IE and non-Class IE wiring, and the susceptibility of the Class IE circuits to noise or electro-magnetic interference (EMI) from the non-Class IE circuits. This concern was formalized as safety position 5.

In response to position 5, the applicant proposed a test program. The applicant has performed a noise immunity qualification susceptibility test on the single channel CPC system. This test determined the susceptibility of the system to EMI. A graph of susceptibility field strengths and corresponding frequencies were established as a baseline. We have reviewed the test procedures, reference 21, and test report, reference 22, and conclude that the noise immunity tests are acceptable subject to satisfactory completion of EMI measurements.

The applicant has committed to measure the actual levels and frequencies of EMI onsite to confirm that these measurements fall within the acceptable range of the baseline graph. The results of the onsite measurements will be submitted in the Startup Test Report. We will review the test report and address our resolution of this item in a supplement to this report.

CEA Position

The CEAs in the reactor core are arranged into 20 quadrantly symmetric sets. Each control element assembly (CEA) has two reed switch position transmitters (RSPT) to provide position information to the CEACs and CPCs. This information is used to calculate planar radial peaking factors in the CPCs and to calculate rod deviation in the CEACs. Our review of the design is presented in the Safety Evaluation Report.

Due to physical constraints in the reactor vessel head area, both Class IE and non-Class IE signals are transmitted within the same cable assembly from the reactor vessel head to a point outside containment. Within this cable assembly, six of the conductors are used for discrete position information, (non-Class IE) which is transmitted to the control element drive mechanisms control system (CEDMCS) and three are inputs to the CPC. For example, Channel "C" has 61 CEAs, therefore, 366 conductors are non-Class IE and 183 are Class IE analog signals that are transmitted to the CPCs. It was noted that all of these conductors are contained in the same raceway, inside containment. Accordingly, the Class IE conductors are dominated by non-Class IE conductors and a concern for noise susceptibility exists. This concern has been expressed as safety position 5.

The applicant responded to the position by proposing a test program. The applicant has performed a noise immunity qualification/susceptibility test to demonstrate that a single event in the non-safety circuits (e.g., "electrical noise") will not degrade the Class IE circuits from performing their safety function. We have reviewed the test procedures, reference 21, and test report, reference 22, and conclude that the noise immunity tests that were conducted on the single channel are acceptable. The applicant has committed to measure the actual levels and frequencies of EMI onsite to verify that the qualification test measurements conservatively bound the onsite measurements. The results of the onsite measurements will be submitted in the Startup Test Report. We will review the test report and address our resolution of this item in a supplement to this report.

D.4.1.3 Core Protection Calculator

Central Processing Unit (CPU)

Our initial review of the CPU is presented in the Safety Evaluation Report. Further evaluation of this component is presented herein.

The CPU has the capability of detecting bit parity errors, check sum calculations and power loss. Upon detection of an error the CPU generates an interrupt that causes the channel to place its output in the trip condition. In addition, each CPC and CEAC includes a watchdog timer utilized for detecting malfunctions in the computer. In the original design, a time-out of the watchdog timer was indicated by means of a status lamp which sealed in and had to be manually reset. Upon observation of the status lamp, the operator was required to analyze the situation and act

accordingly such as bypass or trip of the affected channel. As described in position 23 we require automatic action to trip the CPC upon time-out of the watchdog timer.

In response to position 23, the applicant proposed to implement a hardware and software modification to institute an automatic channel trip upon time-out of the CPC watchdog timer, and the setting of all bits to "1" in the CEAC data link upon time-out of the CEAC watchdog timer. We have reviewed the drawings depicting the hardware and software changes which were made to the CEAC and CPC watchdog timer logic to implement position 23 and conclude that the design meets the Commission's requirements and is acceptable.

D.4.1.4 Control Element Assembly Calculator (CEAC)

CEAC Separation Criteria

Our review and evaluation of the issue is reported in the Safety Evaluation Report. During our review we requested the applicant demonstrate how the output of the optical isolator cards within the CEAC meet the single failure criteria. Card slots 11 through 15 of the MACS Universal Chassis within the CEAC encompass the output cards to channels D, C, plant computer B, and A respectively as shown in Figure D-2 of the Safety Evaluation Report.

All five cards are located within a 3.5-inch section of the chassis. We required the applicant to identify their design basis events for the CEAC and verify that no single event either internal or external to the CEAC will result in the loss of function. Our concerns on this issue are presented as Position 4 in Table D.1.

A failure mode and effects analysis (FMEA) was performed by the applicant in response to this concern. Based on the information provided in the FMEA, reference 23, the effect of a single failure in the CEAC on the CPC was to reduce the auctioneering logic for CEA deviation (penalty factor) to a one out of one in the CPC.

In order to close position 4 the staff requires a satisfactory resolution of position 26. Refer to the next sub-section on optical isolators for more detail on the test results of the application of a credible fault to the optical isolator card that was located in card slot 14. We will address the resolution of this item in a supplement to this report.

Optical Isolators

Our initial review and evaluation of the optical isolators are presented in the Safety Evaluation Report. Our concerns regarding the qualification of the isolators were expressed as position 26. The applicant has responded to the position by proposing a test program for the optical isolators.

We have reviewed the qualification test procedures, reference 24, of the optical isolators and conclude that the procedures were acceptable. The staff also reviewed the test report, reference 25, and concluded that the test results did not satisfy the acceptance criteria stated in reference 24 and is, therefore, unacceptable.

The tests were conducted on the Single Channel CPC System in accordance with test procedures in reference 24. The Single Channel Test System was configured as a CEAC and the 120 volts alternating current (120V AC) fault was applied across the signal lead and the +12 Volt return lead. This fault was directly across the input of the optical isolator located on the input data link card, which was located several feet away to simulate the CPC interface. When the fault was applied to the interface the following events occurred:

- (1) The optical isolator on the input data link card (VBZ1) failed open. This is acceptable. The collector on the output of this device failed open. This failure was confirmed by Aerospace Electronics during their X-Ray analysis of the chip. For further detail, see Appendix A of the test report, reference 25.

This failure does not satisfy Acceptance Criteria 3.2 of the test procedures, reference 24, which states, "When 120 VAC is applied to the optical isolator input lead, no propagation of the fault signal to the optical isolator output shall occur."

- (2) Transistor 2N2367 (card VBZ2) failed open (all three leads), and a hole was burned through the top of its metal can. Examination of Figures 3 and 6 of the test report confirmed that debris was ejected onto the adjacent CFAC output data link board.

This failure does not satisfy Acceptance Criteria 3.4 of the test procedures, reference 24, which states, "There shall be no splashing of molten solder from the data link cards into adjacent printed circuit cards within the multipurpose acquisition control system (MACS) chassis."

- (3) A resistor (560 ohms) on the input data link board associated with the bit being tested burst into flame.

This failure mode was not called out as an acceptance criteria in the test procedures, but is an unacceptable consequence and does not satisfy General Design Criteria 3.

We require that the applicant conform to position 26 and: (a) provide the necessary changes within their design to combat the undesirable failures identified in the evaluation, (b) submit the design changes to the staff for review prior to the rerun of the test, and (c) rerun the test in accordance with test procedures stated in reference 24.

We will review the design change and future test results and address our resolution of this item in a supplement to this report.

The staff has discussed with the applicant the effects of exposure to the optical isolators to radio frequencies (RF) greater than 100 Megahertz (Mhz) upon the response of the CPCS. Our evaluation and concerns regarding this issue are discussed in the Safety Evaluation Report and as safety position 12.

The applicant responded to the position by performing a noise susceptibility test of radio frequencies from 35 MHz through 2GHz on the CPCS. During this test several susceptible frequencies were encountered within this range. However, at each susceptibility point, the CPCS responded in a fail safe manner, i.e., a trip. At the frequency band of the radio transceivers (walkie-talkies) to be used in ANO-2 plant, extended tests were run at power levels up to 17 Volts per meter to verify that the CPCS was not susceptible.

We have reviewed the test procedures and test report, and conclude that the noise susceptibility tests that were run on the optical isolators satisfy the Commission's requirements and are acceptable.

D.4.1.6 Bypasses and Interlocks

In the Safety Evaluation Report we stated that the applicant had identified a CPCS design change to provide a control element assembly calculator (CEAC) operating bypass and that the details had not been submitted for our review. The applicant has provided information describing the function, operation and implementation of the CEAC operating bypass in references 3, 13, 26 and M18. The function of the CEAC bypass is discussed in Section D.3.11 of this report. The operation and implementation of the bypass are evaluated herein.

The CEAC operating bypass has been implemented in the CPC stored computer program as a "CEAC/RSPT inoperable" addressable constant which the operator can enable or disable thru the Operator's Module. The procedure for changing this constant is similar to that used for changing other addressable constants. When this constant is set by the operator, the CPC program will ignore the penalty factors being transmitted from the two CEACs and use a predetermined constant for the penalty factor as described in Section D.3.11 of this report. The CEAC/RSPT inoperable bypass is manually enabled or disabled under administrative controls.

Indication of the CEAC normal (non-bypassed status) or the bypass status is provided by a status lamp on each core protection calculator Operator's Module. We have reviewed the operation and implementation of the CEAC operating bypass and conclude that it meets the requirements of Section 4.12 of IEEE Standard 279-1971 and is acceptable.

In the Safety Evaluation Report, we stated our concern about the potential for initiating false reactor scrams during testing, maintenance and repair of the CEACs and CEA position isolation amplifiers. The concern arose as a result of the functional interaction between the CPCs and the CEACs and the design of the CPCS channel bypass.

The channel bypass provides the capability to bypass one of the four CPCS channels (i.e., the high local power density (LPD) and low departure from nucleate boiling ratio (DNBR) trips) for maintenance or testing. The CPCS bypasses are part of the reactor trip system bypass system provided for each plant trip function. The unique design of the CPCS required that the low DNBR and high LPD trip bypass circuits for CPCS channels B and C be designed with interlocks to channels A and D respectively. The purpose of these interlocks is to enable testing of the CEACs and CEA position isolation amplifiers. The modifications do not affect the bypass and interlock circuits for the six matrix logic networks in the reactor trip system.

Twenty CEA position signals are shared between CEAC channel 1 and CPC channel B and 20 CEA positions are shared between CEAC channel 1 and CPC channel A. (CEAC channel 2 and CPC channels C and D have the same configuration). In addition, the output of each CEAC also provides an input to each CPC. As a result of this functional interaction, we were concerned about the potential repair of the CEACs and CEA position isolation amplifiers. In this regard, we considered the requirement for an additional CEAC channel bypass similar to the CPC channel bypasses. In evaluating the need for a CEAC bypass, we determined that the bypassing of CEACs during test and maintenance would compromise the reliability of the CPCs and the ability of the CPCS to meet the single failure criterion. Thus, although the implementation of a CEAC bypass could improve CPCS operational availability, a decrease in CPCS reliability with respect to performing its safety function could also result. Therefore, it is our opinion that the implementation of CEAC bypass, in addition to the channel bypasses currently provided, would not improve the CPCS capabilities with respect to safety. However, to ensure that the CPCS integrity is sustained during test and maintenance, we required that the detailed procedures describing test and maintenance methods and administrative controls to be used during CPC, CEAC and CEA Position isolation amplifier testing and maintenance be submitted for our review. The applicant provided this information in his response to Position 9. We have reviewed the test and maintenance procedures and administrative controls for the bypass, testing and maintenance of the CPCS. Based on our review, we conclude that the administrative procedures will ensure that CPCS functional integrity is maintained during test and maintenance and that the design of the CPCS channel bypass is acceptable.

D.4.2 Test, Maintenance, Monitoring and Qualification

D.4.2.1 Operational Testing

In our Safety Evaluation Report, we identified several concerns regarding the design, implementation and adequacy of the automatic on-line tests and the periodic tests.

With respect to the automatic tests, we required that the watchdog timer circuits and program be modified. (Positions 21, 22, and 23). The applicant identified additional program design changes to improve the automatic detection of arithmetic overflow and underflow errors. The final designs for the watchdog timer and for the program modifications have been submitted for our review.

In response to staff position 21, the design was changed to make the check-sum (an automatic on-line test parameter) values the same for corresponding blocks in all redundant channels. This was accomplished by setting unused memory locations to zero prior to loading and linking the system software. A secondary benefit is derived from this change because any fault in the system that might attempt to use any of these memory locations will cause an immediate channel trip. This occurs because zero is an illegal instruction in this computer and a fault instruction interrupt causes a channel trip.

We have reviewed the information submitted by the applicant in references M18 and M22. Based on our review we conclude that the automatic on-line test features have been implemented without restricting the primary safety functions of the CPCS and that they provide additional capabilities for detecting equipment failures which do not exist in present designs for analog hard-wired systems. Therefore, we conclude that the automatic on-line testing for the CPCS complies with the staff requirements in safety positions 22 and 23 and is acceptable.

In our review of the periodic tests, we questioned the adequacy of the test procedures and the off-line tests for periodically checking and verifying the functional operation of the CPCS in accordance with the requirements of General Design Criterion 21 and Section 4.10 of IEEE Standard 279-1971. We required that the periodic test program be modified to include procedures for testing each trip function in each channel from sensor input to the CPCS to trip output to the reactor trip system (position 9). The applicant has responded to our position by stating that the proposed periodic tests were based on the overlap testing philosophy and were adequate for verifying the functional operation of the CPCS.

However, it was our position that the proposed overlap tests were inadequate and that a functional operation check from CPCS sensor inputs to the trip output would be required to adequately ensure that the CPCS is operational.

In response, the applicant has committed to performing periodic functional operation checks from CPCS sensor inputs to the trip outputs, reference 32. The test will be accomplished by injecting a test signal for each sensor input at the MACS input/output (MACS I/O) connectors of the CPCs and CEACs and monitoring for trip output when the setpoint is reached. We have reviewed the information provided and conclude that the system functional tests for periodic checking and verification of the CPCS functions meet the requirements of General Design Criterion 21 and Section 4.10 of IEEE Standard 279-1971 and are acceptable.

In our review of the periodic tests, we questioned the basis for the CPCS time interval of periodic testing. The applicant stated that the time interval of 30 days was based on past experience and the test intervals for analog protection systems. However, the CPCS design represents a new configuration for reactor protection systems. In addition, many of the components in the CPCS (digital computers and I/O interfaces, CEA position transmitters, pump speed sensors and CEA isolation amplifiers) are being used for the first time in a protection system. Several are also first-of-a-kind designs. Therefore, we concluded that the past experience with analog protection systems could not be directly applied to the CPCS. We required additional justification of the periodic test interval.

In conjunction with the qualification test report discussed in Section 7A.5.2.5, the applicant submitted an evaluation of the CPCS reliability to justify the test intervals for the CPCS periodic tests and for the CPCS system functional tests in references 35 and 36. We have reviewed the reliability analyses of the CPCS and concluded that the reports do not provide an acceptable basis for establishing the CPCS reliability and test intervals for periodic tests and system functional tests, reference M22.

The use of reliability analysis to establish the initial periodic test intervals is difficult due to the lack of operating experience with digital computer equipment in safety systems applications. The lack of specific regulatory criteria for reliability evaluations and probabilistic analyses in the licensing review of safety instrumentation and control systems further complicates the development of an acceptable reliability analysis of the CPCS. As a result, we have concluded that further reliability analysis at this time will not provide useful information for resolving the initial periodic test interval concerns identified in position 8. We will resolve the concerns regarding periodic testing and functional testing by establishing more conservative test intervals and additional CPCS surveillance requirements in the plant technical specifications until operating experience is gained. This is consistent with the approach the staff has used in previous safety reviews. Based on this technical specification approach, we consider that this matter is resolved.

Our review also identified a concern regarding the off-line periodic test using the predefined data base and calculated results (position 10). We required that the applicant develop practical techniques and procedures for using the off-line program to verify calculated results after changes to addressable constants. The applicant has implemented changes in the CPCS off-line test program and test procedures to automatically accommodate changes to addressable constants when verifying CPCS program calculations. We have reviewed and audited the changes to the periodic test programs and the off-line test procedures described in reference 40. Based on our review, we conclude that the techniques and procedures for using the off-line program are acceptable.

In our Safety Evaluation Report, we discussed the unique design of the CPCS and the reliance on many isolation devices (i.e., optical isolators for CEAC to CPA data transfer and CEA position isolator amplifiers for shared CEA position signals) to maintain electrical independence among the protection channels. As noted, the ability of these devices to maintain the isolation among channels is one of the bases for accepting the design of the CPCS. We identified our concern that failures of the isolation characteristics of these devices would seriously compromise the ability of the CPCS to function. We also stated that the periodic test procedures did not include provision for verifying that the isolation capabilities of these devices have been maintained.

We required that periodic tests be performed to verify the isolation characteristics of those isolation devices used to ensure channel independence (position 27). The applicant has submitted test procedures for periodically checking the isolation characteristics of the CEA Position Isolation Amplifiers and of the optical isolators in references 37 and 38. We have reviewed the test procedures for periodically checking the isolation characteristics of the optical isolators and conclude that they are acceptable as discussed in reference M18. We identified our concern regarding the adequacy of the CEA position isolation amplifier isolation tests. In response to our concerns, the applicant has revised the test procedure, reference 39, to provide a more comprehensive test for periodic verification of the CEA position isolation amplifier input-to-output isolation characteristics. We have reviewed these test procedures and conclude that they are acceptable.

D.4.2.2 Maintainability

In our Safety Evaluation Report, we identified our concerns regarding the maintainability of the CPCS. Previous experience with nuclear power plants, and other industrial uses of process computer systems has identified several concerns regarding maintainability of digital computer systems over the operating life of the plant. These concerns are summarized as follows:

- (1) Lack of standardization in hardware and software design has led to difficulties in identifying second sources of parts supply.
- (2) The short commercial life cycle of electronic parts compared to plant operating life has resulted in obsolescence of equipment and unavailability of spare parts.
- (3) Suppliers and users lack of experienced trained technicians to maintain equipment.
- (4) Incomplete maintenance and trouble shooting procedures and system documentation has made maintenance difficult.

In addition, IEEE Standard 279-1971, Section 4.21, identifies maintainability as one of the requirements for the reactor protection system. In response to our concerns, the applicant provided information describing the procedures for diagnosing CPCS failures. These procedures did not adequately address our concerns regarding the maintainability plan of the CPCS. Therefore, we required that the CPCS maintainability plan be docketed for review and evaluation (position 25). In response to our concern, the applicant has submitted an overall maintainability plan for the CPCS in reference 31. The information identifies maintenance actions, diagnostic and repair features, personnel training and other procedures which will be implemented to ensure that the CPCS can be maintained consistent with the performance requirements of Sections 4.1 and 4.21 of IEEE Standard 279-1971. We have reviewed the information provided and conclude that an acceptable maintainability plan has been established for the CPCS.

D.4.2.3 Plant Computer System Monitoring

In the Safety Evaluation Report, we stated that we required that the plant computer system (PCS) data links to the protection computers be removed and that the plant computer service routine be deleted from automatic program scheduling in the CPCS (position, 20).

In response, the applicant stated his intention to appeal the staff's position. In an effort to resolve our concerns, we proposed in reference 46 a compromise to the original position as follows:

- (1) Only one channel of the Plant Protection System (CPC & CEAC) would be allowed to communicate with the plant computer via a data link. The remaining three channels would not be allowed to communicate to the PCS. The one channel can be manually connected from the PPS to the PCS as AP&L Company chooses.
- (2) This means only 1 CPC and 1 CEAC will be connected to the computer at any one time.

The compromise was proposed on the basis that it would allow the use of the PCS to automatically collect data for use in evaluating and confirming the CPCS design bases analyses and functional performance (the applicant identified this as a primary function of the data links). At the same time, the compromise would resolve our concerns regarding the CPCS independence and acceptably minimize the potential adverse effects of the additional CPCS design complexity required to implement that data link feature.

The applicant rejected this compromise on the following bases:

- (1) The proposed compromise would not allow the significant benefits afforded by the system as presently configured to be realized. Specifically, simultaneous

data from all four CPC channels and both CEAC channels would not be available to support startup and inservice testing; comparison of data from all channels to detect an input or output change or early detection of sensor failure would not be possible; and, the increased periodic test interval by use of the computer would not be possible.

- (2) The staff's bases for not accepting the use of the data links were that the data links "compromise the independence of the protection systems and add an unnecessary degree of complexity to the CPCS design." The proposed compromise in itself would increase the complexity of the design.
- (3) The compromise would have an impact in terms of additional cost and schedule to make the changes noted in item 2 above as well as changing the plant computer software and operating procedures.

An appeals meeting was held on August 16, 1977. At this meeting, information was provided by the staff, reference 48, and their consultant, reference 49, in support of the removal of the data links. The applicant and Combustion Engineering presented information to support retention of the PCS data link feature in reference 47.

In response to the applicant's appeal, the staff's position remained "that based upon General Design Criterion 24 regarding separation of protection and control systems, the data links should be removed," as stated in reference 50. We also stated that we would evaluate alternate CPCS configurations which would allow the data links to be connected between the CPCS and the PCS in a limited manner. The staff in reference 50 identified two possible alternates as follows:

- (1) The data links would be allowed to be connected to all six CPCS computers during startup operations for a sufficient period of time to allow for collection of data prior to the end of the startup testing phase of operations. Similar operation would be allowed on subsequent startups after refueling. To evaluate this alternative, we requested that the applicant provide information describing (a) the specific uses and benefits of the PCS during this period which relied upon the data links; (b) the required duration of operation with the links connected; (c) the procedures for disconnecting the links at the end of this period; and (d) the test criteria and test methodology to be employed to ensure that the data links have been correctly implemented.
- (2) The data links would be allowed to be utilized as described in alternative 1. In addition, at the end of the startup operations, three of the four channels would be disconnected from the PCS with the remaining channel connected and in continuous operation. Rotation of the connection link to the PCS among the four channels could also be done. To evaluate this alternative, the information required to evaluate alternative 1 would also be required. In addition, we stated that we would require that a comprehensive long-term monitoring

program of the data links be implemented to provide data to the staff to demonstrate the reliability of operation of the data links and to quickly detect anomalies or failures, subject to our review and approval. In conjunction with the monitoring program, we stated that we would also conduct a review of the PCS software as it related to the data transmission between the CPCS and the PCS.

The applicant rejected these alternatives, in reference 51, on the bases that neither alternative would accommodate the PCS periodic assessment of CPCS calculations and the PCS surveillance of the CPCS functions. In lieu of the two alternatives, the applicant proposed that all CPC-PCS data links be connected and operable during power ascension and initial commercial operation. During this period, (a minimum of six months at a power level greater than 20 percent), the data links would be intensively monitored according to a pre-determined and mutually acceptable set of criteria and procedures. The acceptability of continued operation of the data links would be based on the outcome of the monitoring program.

We have reviewed the applicant's proposal. Based on our review, we have concluded that this alternate is essentially the equivalent of the original design for the PCS to CPCS data link feature and is, therefore, unacceptable as stated in reference 52. In addition, based on the information provided by the applicant in reference 51, we are assuming that alternate 2, as suggested by the staff, is completely unacceptable to the applicant. Therefore, unless the applicant chooses to reconsider the first alternative - i.e., use of all the data links to collect data only during initial startup and startup after each refueling - and provides the information as required by the staff, we will require that the plant computer data links to the protection computers be removed and that the plant computer service program be deleted from automatic program scheduling in the CPCS.

We will report on the resolution of this item in a supplement to this report.

D.4.2.4 Environmental Qualification

In the Safety Evaluation Report, we identified the following information as required to complete our review of the CPCS equipment's environmental qualification: (a) the analyses demonstrating the radiation exposure qualification of the CEA reed position switch transmitters (CEA RSPT) (position 13); (b) the test results for the thermal qualification tests for the process protective cabinet (position 11); and (c) the test results for the CPCS noise and immunity qualification and susceptibility tests (position 12). The applicant has provided; (a) the analyses demonstrating the radiation exposure qualification of the CEA RPST in reference 27; (b) the test results of the thermal test of the process protective cabinet in references 28 and M19; and (c) the results for the CPCS noise and immunity qualification and susceptibility tests, references M23, 22, and M22. Our review of the CPCS noise and immunity qualification and susceptibility tests is discussed in Section D.4.1.2, of this report.

Based on our review of the information provided to demonstrate the radiation exposure qualification of the CEA RSPT, we conclude that the CEA RSPTs meet the environmental qualification requirements for radiation exposure and are acceptable.

Based on our review of the results of the thermal tests of the process protective cabinets, we conclude that the environmental conditions within the process protective cabinets will be maintained within the minimum CPCS environmental design conditions for the maximum ambient environmental design conditions in the plant area where the plant protective cabinets are installed. On this basis, we conclude that the CPCS equipment housed in the process protective cabinets meets the environmental qualification requirement and is acceptable.

In the Safety Evaluation Report, we noted that the acceptability of the qualification of the CPCS sensors (CEA RSPTs and RCP speed sensors) located inside containment was dependent upon our review of qualification of Class IE equipment for operation during and following the main steamline break accident. Based on our review of the information in the applicant's Final Safety Analysis Report, we have concluded that these CPCS sensors are not required to operate during and following the main steamline break (inside containment) accident. The applicant has provided environmental qualification test results for the CEA RSPTs and RCP speed sensor in references 29 and 30. Based on our review of the environmental qualification tests results, we conclude that the CEA RSPT and RCP speed sensors are qualified to operate and will perform their function while exposure to the maximum design environmental conditions in which they are required to function. On this basis, we conclude that the environmental qualification of the CEA RSPT and RCP speed sensors is acceptable.

D.4.2.5 Seismic Qualification

Our review of the seismic qualification of the CPCS is also reported in the Safety Evaluation Report. Our safety concerns regarding seismic qualification are stated as position 14 of Table D.1. As noted in Table D.1, position 14, the staff requested that the applicant provide additional information to verify the adequacy of the seismic loads used for testing the CPCS equipment housed in the process protective cabinet (PPC). Information to support the ability of the PPC and computer to survive the seismic events has been submitted and is currently under review.

D.4.2.6 Pre-Operational Test

The staff solicited the services of a test consultant in the evaluation of the applicant's Pre-Operational Test Program and Startup Test Program. For the Pre-Operational Test Program, the test consultant evaluated the test procedures for the CPC and the CEAC calculator subsystems. The evaluation concluded that the test procedures were incomplete to verify installation of the system. Accordingly, the test consultant recommended the execution of failure-response type tests. For example, a failure-response test verifies that the detection of a failed sensor is

as designed, and that the operator is alerted through a status lamp or an alarm as required. These recommendations have been forwarded to and discussed with the applicant as stated in reference 41.

The applicant has committed to conduct failure-response tests desired. Subject to an evaluation of the final test procedures and of the test report, the staff considers the concern resolved.

D.4.3 Software Design Evaluation

D.4.3.1 General

An overall review of the ANO-2 CPC software was presented in the Safety Evaluation Report. Therein the specific guidelines and criteria for reviewing the system software were discussed. It was further noted that documentation of the functional design description was still under review and final documentation on software specifications and program listings would not be available for review until a later date. The final documentation for the software review has been completed and is the subject of this review.

The final software submitted for the ANO-2 CPCS is comprised of the following programs:

<u>Program Name</u>	<u>Revision No.</u>	<u>Date</u>
(1) CPC/CEAC Executive System	2.01	7/22/77
(2) Primary Coolant Mass Flow Program	2.05	7/15/77
(3) Primary Coolant Mass Flow Constants	2.05	7/21/77
(4) DNBR Update Program	2.08	7/15/77
(5) DNBR Update Constants	2.06	7/15/77
(6) Power Distribution Program	2.01	7/15/77
(7) Power Distribution Constants	2.01	7/15/77
(8) Static DNBR Program	2.01	7/15/77
(9) Static DNBR Constants	2.01	8/3/77
(10) Trip Sequence Subroutine	2.02	7/15/77
(11) Trip Sequence Constants	2.00	7/15/77
(12) Common Subroutines (FIX, ALOGX, EXP)	2.01	7/15/77
(13) CPC Global Data Base	2.01	7/15/77
(14) CPC Executive Data Base Overlay	2.01	7/15/77
(15) CPC Point ID Table	2.00	7/15/77
(16) CPC Gain/Offset Tables	2.01	7/15/77
(17) Penalty Factor Program	2.01	8/3/77
(18) Penalty Factor Constants	2.01	8/3/77
(19) CEA Position Display Program	2.01	7/24/77
(20) CEA Position Display Constants - CEACT	2.01	7/24/77

	<u>Program Name</u>	<u>Revision No.</u>	<u>Date</u>
(21)	CEA Position Display Constants - CEAC2	2.01	7/24/77
(22)	CEAC Executive Data Base Overlay	2.01	7/24/77
(23)	CEAC Point ID Table	2.01	8/3/77
(24)	CEAC Gain/Offset Tables	2.00	6/27/77

The basic design of the CPC software has not been greatly altered from the original description. However, a number of changes were made by the applicant and reviewed with the staff. A majority of the changes were initiated by the designer to reflect modifications to the original functional specifications. Generally, they may be classified as program improvements to better accomplish the same task. Two or three changes resulted from non-critical errors in the original programming. Several changes were made in response to staff positions or recommendations. Also, the experience gained during Phase II testing of the "Frozen Design" resulted in several design improvements in the man-machine interface.

D.4.3.2 Documentation

The final design description provided by the applicant for the ANO-2 software has been reviewed for documentation adequacy. The audit principle was applied to selected programs from the functional design description through final assembly language listings, including selected core dumps. Based on the audit we have found the material to be well organized and presented in a clear and concise manner. The designer has incorporated many descriptive comments in the final assembly listings. This has greatly improved the traceability of the intended functions of the programming. An independent reviewer familiar with assembly language programming conventions should be able to trace the design from the engineering descriptions through the final implementation. However, one potential area for confusion was detected during our review and should be noted because of its potential adverse impact on future software maintainability. The problem relates to the manner of indexing or sub-scripting multidimensional variables. In many equation statements in the functional descriptions the FORTRAN convention is used wherein the lowest allowable index is the number "1." When the equations are represented by logic diagrams for the programmer specifications the assembly programming convention is often used wherein the numeral zero represents the lowest allowable index for dimensioned variables. This generic type program has no simple fix because a change in the assembly index to make it consistent with the FORTRAN representation results in an inconsistent dimension statement. Our audit found no errors in the existing documentation relating to indexing.

The applicant's software specifications include program descriptions, requirements, flow charts, equations and values of constants. The software specifications are generally consistent with the functional description in references 3 and 4 and data base document, reference 5. A major difference between the specifications and functional description lies in the time execution requirements for each program.

Specification timing requirements for the Primary Coolant Mass Flow Program, DNBR and Power Density Update Program and Power Distribution Program are not consistent with timing requirements given in the functional description and used for deriving data base constants. The longest acceptable execution interval is given in the functional description for each of these programs. Specification timing requirements for the Static DNBR and Power Density Program are not consistent with the timing requirement given in the functional description and verified by test. The longest acceptable execution time interval for the static program is given in the functional description.

With the exception of the algorithm execution intervals discussed above, the software specification defines an acceptable system. With the algorithm execution intervals specified in the functional description, the software specification is acceptable as a specification for the CPCS.

D.4.3.3 Quality Assurance

The staff's evaluation of the quality assurance program description consisting of design control, manufacturing and certification testing for the core protection calculators was previously reported in the Safety Evaluation Report. The report described the quality assurance program as acceptable except for the evaluation of the program's implementation to be conducted at a later date.

The quality assurance procedures have been greatly improved since our last audit reported in reference 1. The designer also provided an improved means for monitoring the operating system for changes to the core memory. This was accomplished by adding the capability of reading the check-sum values via the Operator's Module. This design feature provides a definitive method for independent auditors to reassess the software quality and guard against unannounced changes to the core memory. The check-sum automatic audit program provides continuous on-line protection against hardware failures that cause memory faults as well as protection against unauthorized attempts to change any program. We have independently analyzed the CPC and CEAC memory dumps and concur with the check-sum values for each block of memory as reported in reference 12.

The Office of Inspection and Enforcement (OIE) of NRC has conducted an inspection to verify implementation of the quality assurance program for software design verification and qualification of software changes as conducted by Combustion Engineering in the design of the CPCS. Based on their inspection report, reference 11, the Office of Inspection and Enforcement concludes that the implementation of the quality assurance program for software design verification and qualification of software changes is in accordance with the quality assurance program description of the CPCS, and complies with the requirements of safety position 16.

D.4.4 Software Qualification

Our initial evaluation of software qualification is presented in the Safety Evaluation Report. Subsequent to our safety evaluation, the applicant initiated a redesign and a requalification effort for the computer programs. Sections D.4.4.1 thru D.4.4.4 presents our evaluation of the Phase I and Phase II requalification test program. Section D.4.4.5 presents our review to date of the startup tests, which will be used to verify and evaluate the conservatism of physics and thermal hydraulic computer program data base constants for the system. Finally, section D.4.4.6 presents our evaluation of the single channel test system, which is to be used for requalification tests after software modifications have been made.

D.4.4.1 Phase I Test Plan

The purpose of Phase I testing was to verify the implementation of the core protection calculator system (CPCS) software. Implementation is defined as the translation of the system functional requirements into modules of machine executable code, and the integration of the code modules into a realtime software system. An additional objective of the input sweep test supplement to Phase I testing was to determine the overall uncertainty associated with the implementation of the algorithms on a 16 bit machine versus a 32 bit machine.

Within Phase I testing, two levels of testing were performed; one at the module level and one at the program level. At the module level, sufficient test cases were run to exercise every functional branch in the module. Modules whose inputs included a selection index to select constant values from a table or array of constants were tested with sufficient cases to exercise all values of constants in the table. Test cases at the program level were chosen to be representative of conditions which the program is expected to experience in service.

The input sweep tests were run to:

- (1) Determine the processing uncertainties of the algorithms as coded on the Interdata Model 7/16 Computer,
- (2) Verify the ability of the CPC algorithms, as coded on the Interdata Model 7/16, to initialize to a steady-state after an auto-restart for each of a large number of input combinations within the CPC operating space.
- (3) Complement Phase I and Phase II testing by identifying any data dependent abnormalities in the CPC algorithms coded on the Interdata Model 7/16 which were not uncovered previously; and to demonstrate that any such abnormalities result in a safe CPC response such as a channel trip if arithmetic overflows or underflows are generated.

The input sweep test exercised each CPC algorithm over and beyond the range of sensor readings expected to be encountered during operation. The independent variables that characterize reactor operating conditions (e.g., core inlet temperature, power level, pump configuration) were specified, as well as the steady state transfer functions that relate the independent state variables to the CPC sensor readings (e.g., hot leg temperature is a function of cold leg temperature, power, pressure, etc.). The input sweep test program calculated the CPC sensor inputs for a set of reactor operating conditions based upon the transfer functions. These sensor inputs were then substituted into the CPC data base as sensor readings and the computer program was then executed. Once the CPC outputs had stabilized, the sensor input values and a selected set of calculated results were output to a data tape for off-line comparison with previously determined results from the CPC FORTRAN code.

D.4.4.2 Phase I Test Results

In the evaluation of the test program, the staff conducted an audit of the test execution and evaluated the test report submitted by the applicant. Our evaluation of the test audit is presented in reference M17. The applicant addressed these concerns in the Phase I test report, reference 19. Our evaluation of the Phase I test results are presented below.

During the initial Phase I test program, three software coding errors were discovered.

- (1) Four constants in the shape annealing matrix (SAM) array had been scaled incorrectly for Module 5 of the Primary Coolant Mass Flow Program.
- (2) An error in the System Monitor Task prevented a few unused portions of the disk buffer from being copied to the core in preparation for periodic testing.
- (3) A constant in the AIJ array which is used in Module 2 of the Static DNBR Program was implemented incorrectly.

Software Change Requests were initiated to correct the errors described in items 1 and 3 above. Upon completion of the software modifications, the affected modules were retested and produced satisfactory test results. Item 2 will be corrected by a revision of the specification as system performance is not affected. Also, errors detected in Phase II tests were corrected and the affected Phase I tests were rerun to assure that the corrections did not induce further error.

The input sweep tests consisted of 2000 test cases in three sub-sets. Sub-set 1 consisted of 900 cases which covered four pump operation. Sub-set 2 consisted of 420 cases which covered part loop operation. Sub-set 3 consisted of 680 cases which covered penalty factor cases during four pump operation.

For each test case, the difference between the FORTRAN code results and the CPC Interdata Model 7/16 results was calculated. Certain sweep cases had departure from nucleate boiling ratio (DNBR) differences which exceeded E_1 , the allowable error criterion. The staff required the applicant to review all test cases wherein the difference was greater than E_1 . We reviewed the magnitude of E_1 and found it to be acceptably small and consistent with the test criteria and the test conditions. A small number of the sweep test cases had DNBR differences greater than a value which shall be designated as E_2 .

All cases with DNBR differences greater than E_2 had differences in the axial shape index. The CPC treats a node as unrodded if a control element assembly (CEA) is located at or above the center of the node. Because of computer word truncation, the CPC FORTRAN code treats a node as rodded if the raw CEA position is at the node center. An analysis was performed with the CPC FORTRAN code modified to simulate the CPC treatment. Much better agreement resulted.

Subsequent to the noting of CEA position effect at node centers, additional analysis of the test cases with DNBR differences greater than E_1 indicated that the CPC system core average heat flux was not equal to the core average power for static power levels. A study indicated that the dynamic compensation filter did not have a gain of one for steady-state operation. This effect did not occur for the CPC FORTRAN code.

The heat flux dynamic compensation filter error is the result of different computer word accuracies of the Control Data Corporation Model 7600 computer (CDC 7600) (a 32 bit computer) on which the CPC FORTRAN code is run, and the Interdata Model 7/16 (a 16 bit computer) which is used as the CPC. This is a true processor uncertainty which is not included in the ANO-2 data base but must be incorporated prior to startup. An acceptable approach is to include it in one of the addressable constants utilized to accommodate uncertainties in the power and heat flux terms. To further examine this effect, the heat flux dynamic compensation filter was modeled on an Interdata Model 7/32.

Extracting the effects of the CEA position and heat flux filter characteristics resulted in an approximately normal distribution of DNBR differences with a very tight band of differences. The statistical distribution of DNBR differences is characterized in the Phase I Test Results report, reference 19.

The staff finds that Phase I testing was a satisfactory verification of the implementation of the power distribution algorithm software. Each branch of each power distribution module and each component of the radial peaking factor table in the CPC software were tested by a comparison of results from the FORTRAN code and the CPC machine language computer codes wherever possible. For a few cases, verification of the CPC software was by hand calculation. Because of the satisfactory verification

of the implemented code, our concerns regarding position 24F have been resolved through an audit of test results. The staff concludes that the goals of the Phase I tests, including input sweep tests, have been met and that the results of the Phase I testing are acceptable.

D.4.4.3 Phase II Test Plan

The staff has reviewed the Phase II test plan, including acceptance criteria for test results, which is described in CEN-55(A)-P, reference 17, and Supplement 1-P of that document. The primary objective of the Phase II testing is to verify that the CPC and CEAC algorithms have been properly integrated with executive software and the system hardware. Each of the system components are verified by separate Phase I testing and by Hardware Qualification Testing prior to testing of the integrated system.

The test plan of CEN-55(A)-P, reference 17, was applicable to testing of the final ANO-2 software. The initial Phase II test as reported in CENPD-222-P, reference 53, was unacceptable to the staff and the staff requirements for an acceptable test program were defined by position 24. Our review of the Qualification Test Procedure included an evaluation for consistency with position 24 requirements.

The Phase II test program consisted of thirty six static test cases comprising a representative set of steady-state operating conditions and twenty six dynamic test cases consisting of a representative set of CPC design basis events, anticipated plant transients, and artificial single parameter transients. Acceptance criteria for the Phase II tests are defined based on a comparison of the CPC system response to the response predicted by the CPC FORTRAN Simulation code of the CPC software for corresponding test cases. The acceptance band includes a tolerance for steady-state variations as described in CEN-55(A)-P, reference 17.

The magnitudes of the expected ranges for each test case was quantified based on detailed analyses of the above effects, including runs for each test case on the CPC FORTRAN Simulation Program. The CPC processor uncertainty was obtained by comparison of input sweep test results obtained on the Windsor Single Channel Test Facility versus those obtained from the execution of the CPC FORTRAN Simulation Program.

The range of acceptable trip times for Dynamic test cases is determined by the effects of the uncertainties considered for the static test cases plus the time offset for initiation of the transient in relation to the start of a CPC or CEAC computational cycle. The latter effect is large in comparison to other uncertainties.

In response to staff positions, analyses were performed for five selected dynamic test cases using Combustion Engineering design codes to determine the latest trip time required to prevent DNBR of less than 1.3. The analysis was not provided for

dynamic Case 3, one out of three reactor coolant pump loss of flow, since the system is not being qualified for part loop operation. This analysis must be submitted if the system is to be qualified for part loop operation.

Also in response to staff positions, a time history analysis of the CPC DNBR margin and LPD margin was obtained from the CPC FORTRAN Simulation Program to determine the range of time history response for five single parameter dynamic test cases.

The staff finds the test plan acceptable and responsive to staff position 24G.

D.4.4.4 Phase II Test Results

The staff has reviewed the Core Protection Calculator Phase II Test Report, reference 18, for qualification of ANO-2 final design software. The staff also conducted an audit of the Phase II test as described in reference M18. The Phase II test program was performed in its entirety to supercede the earlier Phase II testing of "frozen" design software which was unacceptable to the staff. The functional design description and data base for the final design software are described in references 3 and 5. Phase II testing was performed in August, 1977, at System Engineering Laboratories, Fort Lauderdale, Florida.

Preliminary analysis of the Phase II test results revealed some deficiencies in the modeling of the system to generate the acceptance criteria reported in reference 17. The tolerance bands of expected values were revised to reflect refinements in the simulation of the Power Utility Plant Simulator (PUPS) function, modeling of noise, and application of the input sweep test results. The staff has reviewed the test results in comparison to both the original range of expected values reported in the test plan and the revised range of expected values provided in the Phase II test report. We conclude that the adjustments are small and facilitate the analysis of test results without prejudice to the conclusions, and are, therefore, acceptable.

Test results for DNBR values in 20 of the 36 static test cases were outside of the acceptance range on one or more CPC channels, and required further analysis and explanation. Most of the out-of-range cases were attributed to noise amplitude either greater (low out-of-range) or less (high out-of-range) than assumed when computing the expected values. Four cases were further biased on the high out-of-range side by deviations in the Power Utility Plant Simulator (PUPS) analog outputs with higher values than expected as discussed in reference 17. All static cases which were outside of the acceptance range were rerun on the Windsor Single Channel Test Facility and results were compared to outputs on the CPC FORTRAN Simulation Program for a noise amplitude of zero on all inputs. The DNBR results were in close agreement and are acceptable to the staff.

Peak local power density (LPD) results were within the expected ranges for 30 of the 36 static test cases. As for the DNBR results, noise was the primary factor responsible for the six out-of-range cases. This was confirmed by running these cases on

the Windsor Single Channel Test Facility with fixed inputs. We conclude that in all cases, the single channel result and CPC FORTRAN Simulation Program results were in acceptably close agreement.

As for the static test cases, initial measured DNBR values for dynamic test cases were affected by noise and PUPS output values different from those assumed when computing expected test results. Only five of the 26 dynamic test cases were within the expected range for initiation of the transients. Out-of-range local power density (LPD) values were observed in four of the 26 dynamic test cases. Deviations were attributed to noise characteristics of the PUPS system and PUPS analog output uncertainties.

Sixteen of the 26 dynamic test cases met the acceptance criteria for time to trip or reset in all four channels. Out-of-range results for seven cases, were shown to be due to noise and output uncertainties with the PUPS system.

Two cases, 23 and 25, were affected by fast central processing unit (CPU) clocks in CPC channels A and B. The system surveillance performed during the Software Burn-In Test revealed that the clocks which generate the interrupt signals were running fast, resulting in interrupts occurring at a 10 percent faster rate than intended. The impact of the increased interrupt rate on Phase II testing was analyzed and found to be small with significant impact only on the two cited cases. The dynamic algorithms include derivatives based on the design sampling rate; fast interrupts affect the sampling rate and result in erroneous derivative calculations. The cause of the problem was traced to faulty integrated circuits on CPU clock boards; the circuits have since been repaired. The periodic test is designed to test the clock and detect anomalies of the type described above.

Test Case 14 which was also out-of-range, is a 100 percent to 90 percent step power decrease which results in DNBR increase with no trip output during the transient. Expected results were based on the final time at which the DNBR increases above 2.2. The DNBR did increase above 2.2 at approximately the expected time but dropped below that value much later in the transient (50 to 65 seconds) due to a series of downward spikes in DNBR. This was attributed to effects external to the CPC/CEAC system after extensive analysis of the case failed to reveal any software errors.

Dynamic test cases 17 through 22 are single variable transient tests. The time history of the DNBR and LPD output response compares well to the same cases performed on the CPC FORTRAN Simulation.

Analyses were performed using design codes to determine the trip time response necessary to preclude violation of fuel design limits for five relatively limiting design basis events. The actual trip times obtained with the CPCs provided substantial margin over the trip times required.

Conclusions - Phase II Test Program

The staff review of the Phase II test program includes an evaluation of conformance to pertinent staff positions and previous commitments. We find that Position 17 requirements for Performance Qualification Testing have been satisfied by the Phase II test program and this issue is resolved.

Position 24 staff concerns have also been reviewed and the present status follows:

Position 24A - The staff concludes that the Phase II test program is acceptable for verification of the correct implementation of the final design software.

Position 24B - Changes to the "frozen" design software have been documented and justified by the applicant, including a CEAC software correction and modification to one erroneous DNB constant which was discovered at the start of the current Phase II testing and reported in reference 15. The staff finds the documentation of software modifications acceptable.

Position 24C - The time history analysis provided in the Phase II test report is acceptable for resolution of this staff concern.

Position 24D - The Phase II test report did not directly address concerns with dynamic test case 15 results during Phase II testing of "frozen" software. However, the satisfactory results of final software testing for this case are acceptable to alleviate this concern.

Position 24E - The analysis of dynamic test cases presented in the Phase II test plan and test report are acceptable for resolution of this position.

Position 24F - Our evaluation of conformance to this issue is discussed in Section D.4.4.2. The applicant has successfully resolved our concerns on this issue.

Position 24G - The Phase II test plan resolves this staff requirement.

Position 24H - The applicant has provided an analysis of the problem defined by this staff position. The attachment to a recent Arkansas Power and Light Company letter, reference 54, contains an acceptable resolution of the CPC failure witnessed by the staff on November 25, 1975. The software change and subsequent testing provide adequate assurance that the deficiency has been corrected.

Position 24I - Static test acceptance criteria in conjunction with the analysis provided in the Phase II test report are acceptable for resolution of this concern.

Position 24J - Dynamic test acceptance criteria included transient analyses using design codes for selected test cases as required by this position. The results are acceptable.

Position 24K - Phase II test results for final design software indicate that previous scaling errors have been resolved.

Position 24L - Software changes and subsequent testing have adequately resolved this concern.

Position 24M - Software changes and subsequent testing have provided acceptable resolution of the recurring auto-restarts problem.

Position 24N - Dynamic test cases have been repeated as required by this position.

The staff finds the final design test results acceptable, subject to a satisfactory software burn-in test. We conclude that all aspects of position 24 are resolved.

Although the integrated system test results are acceptable for qualification of the final design ANO-2 software implementation, the staff remains concerned about the effects of process noise on CPCS performance. The difficulties encountered in predicting the noise effects and the apparent sensitivity of the power calculations to the dynamic component of the thermal power algorithm are examples pertinent to staff position 12. We will require that the applicant fully evaluate the impact of process noise on CPCS performance during the startup testing program. Position 12 will remain outstanding until such an evaluation is complete. The requirements for the resolution of position 12 will be stipulated in a condition to the operating license.

D.4.4.5 Integrated System Burn-In Test

During review of the CPCS, the staff expressed concern on the new and unique systems that were being utilized for the first time in a protection system. We required at that time a three- to five-month burn-in test be conducted on the total integrated system. The applicant responded with a proposed three-month test to demonstrate the qualification of the integrated design. The test procedures in reference 33 were submitted, reviewed and found acceptable to the staff.

The staff conducted an audit of the hardware burn-in test as discussed in reference M15 on February 10-11, 1977 and performed several ad-hoc tests in order to evaluate the system response. The results of the ad-hoc tests were acceptable.

The staff has reviewed the Qualification Test Report, reference 34 and found it acceptable for a burn-in test of the hardware, but not as a basis for demonstrating reliability of the integrated system.

The staff position 18 requires a burn-in test of the integrated system. The staff agreed that the three-month hardware burn-in test could be conducted with frozen design software provided that a software burn-in test of minimum two weeks duration

was conducted with final designs software in conjunction with the Phase II testing. Procedures for this test were described in CEN-60(A) dated July 22, 1977.

The staff performed an audit of the Phase II test and the software burn-in test on August 8-9, 1977 and the audit results are discussed in reference M18. The test had been initiated on July 25, 1977. As a result of the audit, the staff found that the Software Burn-In Test did not conform to stated test procedures and experienced several hardware and software anomalies requiring modifications to the system. It was concluded, as stated in reference 55, that the results of the Software Burn-In Test were unacceptable for resolution of position 18. The applicant was advised that to resolve position 18, the staff will require a successful integrated Burn-In Test of the Core Protection Calculator System. The test is to be conducted with test procedures acceptable to the staff, and is to be executed prior to startup of the plant. The test results, which are to be presented in a test report, must demonstrate the functionability of the integrated system, consistent with the General Design Criterion for Protection Systems, as expressed in Appendix A of 10 CFR Part 50.

The applicant responded by proposing retest of the system at the ANO-2 site for a two-week duration in accordance with procedures described in reference 57. The staff reviewed these procedures and stated several comments and concerns in a meeting with the applicant on October 28, 1977 as discussed in reference M20. The applicant further responded to staff concerns with revised test procedures as described in reference 56. Acceptance criteria included in reference 56 require that the burn-in test be reexecuted for a two-week period if any abnormal operation requiring modification of the hardware or software design should occur during the test. The staff has reviewed these revised test procedures and finds them acceptable provided that the following modifications and amendments are made and executed:

- (1) Under section 5.2 of the test procedure, the requirement of a periodic test and software diagnostics at the end of the two-week period to verify that no changes have taken place should be added.
- (2) Under section 1, the purpose should be expanded to state that all abnormal operation will be recorded and evaluated for the cause of the abnormality.
- (3) Table 1 of the test procedures defines the software for the Integrated Burn-In Test. This table is to be amended with the definition of the discs used to initially load the system. Also, describe the procedures used to quality assure the discs. Finally, relate these disc's to the disc's that were used for the Phase II test.
- (4) Upon completion of the subject tests, the results are to be analyzed and a test report is to be generated. The test report is to be submitted for staff review.

Position 18 remains outstanding pending the performance of an integrated system burn-in test in accordance with reference 56 and submittal of a test report acceptable to the staff.

D.4.4.6 Qualification of the Single Channel Test System for Testing of Future Software Modifications

CPCS Position 19C requires that the core protection calculator (CPC) assembly language program be subjected to static and dynamic tests on an acceptable test system. The test program is to include sufficient reactor simulated transient test cases, static test cases, and single variable transient test cases to demonstrate that results from the CPC assembly language program agree with results from the CPC FORTRAN Simulation program for corresponding test cases. For ANO-2 software, this position was satisfied by the Phase II test program conducted on the plant system as configured on the Systems Engineering Laboratory test bed.

The applicant has requested that the Combustion Engineering Single Channel System at Windsor, Connecticut be qualified as an acceptable test system for future CPC software modifications.

The test report, reference 20, describes the test program conducted to qualify the Windsor Single Channel Test Facility as an acceptable test system for CPC software modifications. The CPC FORTRAN Simulation program was used to determine expected results for five static and five dynamic test cases.

The acceptance criteria for the static test cases were generated through the evaluation of the impact of test channel properties (noise, processor uncertainty etc.) with the FORTRAN Simulation program. For all static test cases, the single channel test results fell within the acceptance criteria bandwidths.

The acceptance criteria for the dynamic test cases were generated through the evaluation of the impact of execution properties (time offset) and test channel properties (noise, processor uncertainty, etc.). Each dynamic test case was executed ten times on the single channel facility and results recorded. In all cases, the dynamic test results fell within the acceptance criteria.

The test program did not include multi-variable transient test cases. The single channel system, as configured, did not have the capability to execute multi-variable test cases.

For all test cases executed, only the Core Protection Calculator was exercised. There is no evidence to indicate that the Single Channel Facility is qualified for conducting software modifications to the Control Element Assembly Calculator (CEAC) or to the interfaces between the calculators. A program to address this concern was defined in reference 53, but has not been implemented.

Positions 19D and E provide for transfer of software from an acceptable test system to the plant system when a Phase II type test program is performed in an intermediate test system. Static and dynamic test cases were to be performed on both systems to demonstrate that the two systems are equivalent and that the procedures for transfer from one system to the other are adequate. Performance of these test cases on both systems is required only once for qualification of an intermediate test system for use in software change procedures.

For the Windsor Single Channel Test Facility, the staff agreed to accept five single variable transient test cases and five static test cases as the bases for qualification of the single channel system as an acceptable intermediate test system. These tests were performed on both the single channel system and the plant system as configured at Systems Engineering Laboratory. Results from each of the test series were evaluated by comparison to acceptance criteria generated with the CPC FORTRAN Simulation program, but were not compared to each other as required by Position 19D.

The staff has reviewed the single channel test results and compared them to results of the same test cases observed during the Phase II audit as discussed in reference M18 and results stated in the Phase II Test Report, reference 18. Some observations are as follows:

- (1) For static test cases 1, 2, 3, 21, and 33, results for DNBR were comparable between the single channel and plant systems and compared well to the FORTRAN results. There were no trends evident to indicate that results were affected by differing noise or other characteristics of the two systems.
- (2) For dynamic test cases 17, 18, 19, 20, and 21, the acceptance criteria bandwidths, which included the effects of noise, were comparable even though the noise variance was greater on the PUPS system. Likewise, the bandwidth of test results were comparable for the two systems, indicating that noise effects are masked by the other factors causing a variance in test results. However, the time-to-trip measured on the PUPS system showed a clear trend towards longer trip times with several out-of-range values on the high side of the acceptance band.

The staff believes that the non-conservative trend of results on the PUPS system compared to the Single Channel System is sufficient to warrant direct comparison and explanation before the Single Channel System can be accepted as characteristic of the plant system.

It is also noted from the Single Channel Qualification Test Report, reference 20, that for all of the static and dynamic test cases reported therein, the high auctioneer selection of power was not exercised. This is not representative of the system proposed for licensing. Operation of the system in this manner violates the design bases for the system.

In order to resolve the above concerns and complete our evaluation of the single channel system for testing of future software modifications, the staff will require the following:

- (1) Additional analyses supported by test data must be supplied to confirm that differences in time-to-trip for dynamic test cases run on the single channel system versus the plant system in the Phase II test configuration are due to anomalies in test case inputs or similar causes not pertinent to the software change procedures and not indicative of different response characteristics of the two systems.
- (2) An acceptable test program must be implemented to demonstrate that the single channel system is a qualified test system for:
 - (a) Testing of Interfaces between the CEAC, CPC, and Operator's Module,
 - (b) Execution of either option for high power selection, and
 - (c) Testing of multi-variable transients.

The above requirements relate to utilization of the single channel test system as the test bed for final qualification testing of modified CPC software in accordance with staff Position 19C. ANO-2 software must be subjected to a complete test program on the plant system after any program modification until an intermediate test system has been fully qualified. The test configuration and test program for testing on the plant system are also subject to approval by the staff.

The applicant has taken exception, as discussed in reference M24, to Position 19E which states that all software design changes and revisions to constants in memory (except addressable constants) are subject to documentation, review and approval by the staff. The applicant stated that it is their intent to make changes to the computer program and to submit for the staff's review only those changes that they consider to be a safety issue, e.g., if the margin of safety, as defined in the basis for any technical specification is reduced. Changes such as adjustment of a pre-trip alarm limit would not be reported.

The staff has considered the position of the applicant with respect to 19E. We shall require that all software changes (change is defined as any modification requiring regeneration of the disk) be fully qualified in accordance with change procedures, including a test system and test program, which have been accepted by the staff. All changes in program logic will be subject to prior approval and review by the staff on a case-by-case basis. With respect to the applicant's position, other changes which the applicant believes to be nonsafety-related will be permitted without prior approval of the staff; such changes are to be categorized in advance and a test program acceptable to the staff is to be defined in advance. The test program must be broad enough in scope to provide reasonable assurance that the software modifications will not result in errors or unexpected effects on the

functional performance of the CPCS. We shall require that a master disk of the immediately preceding version of CPCS software be retained. Examples of changes for which pre-defined test programs could be acceptable would be selected groups of data base constants which are non-addressable from the operator console.

Position 19 remains outstanding. If an approved change procedure does not exist prior to licensing, a license condition will prohibit changes to the qualified ANO-2 software until a change procedure has been fully qualified in accordance with position 19 and accepted by the staff. Technical specifications will address the software change restrictions and will require that all changes be documented and submitted to the staff.

D.4.4.7 Startup Tests

The adequacy of the design implementation of the CPCS is verified by design qualification testing. Certain assumptions made during this process require further verification based on data obtained during the plant startup testing. Although the tests are similar to tests in plants with conventional analog protection systems, the data required during the tests and method of analysis of that data have been modified in some areas to be compatible with the CPC design.

The staff has assessed the startup test requirements as stated by the applicant in reference 6 and is in the process of evaluating detailed test procedures. Our assessment of the startup test requirements as well as those of a test consultant are presented in the following paragraphs. Our evaluation of the detailed test procedures will be presented in a supplement to this report.

For verification of reactor coolant Mass Flow Algorithm constants, pump speed will be input to the CPC's during hot functional testing with three of the CPC's simulating 50 percent 80 percent and 100 percent power conditions. Calculated normalized core mass flow rates will be compared with measured normalized core mass flow rates. If required, addressable calibration coefficients will be adjusted to produce agreement or a conservative bound between calculated and measured mass flow rate. This method is acceptable for verification of the forward flow coefficients for each loop but will not adequately characterize the reverse flow coefficients. The reverse flow coefficients must be verified by acceptable reactor tests as a necessary condition for part loop operation.

The thermal power coefficient will be determined at steady-state power levels of 20 percent 50 percent 80 percent and 100 percent during the power ascension test program. The adequacy of the power adjustment coefficients to compensate for power dependent uncertainties in the CPC measured static thermal power will be tested. If all the values of the thermal power adjustment term are in the band -0.5 percent to +0.5 percent of rated power, then the current values of the thermal power adjustment coefficients are acceptable and no further action will be required. If any of the

values are not within this band then the coefficients must be reevaluated. Until the reevaluation is complete, the power must be recalibrated after changes of more than 20 percent of rated power. This method of determining the thermal power coefficient and verifying the thermal power adjustment coefficients is acceptable to the staff.

A independent consultant to the staff has also evaluated the startup test program. A review of the startup test requirements that are presented in reference 6 was conducted. A discussion of the testing methodology and acceptance criteria is presented by the consultant in reference 44. An evaluation of detailed test procedures is also being conducted, the results of which will be presented in a supplement to this report.

TABLE D.1

CORE PROTECTION CALCULATOR SYSTEM POSITIONS

A listing of the staff positions that developed during our evaluation of the CPCS is presented below. Each position's number and title is followed by either a section number of this report or a reference to the previous SER, in which further detail on the position is presented. The current status of the position is also stated. We will report our further evaluation of the outstanding issues in a supplement to this report.

(1) Uncertainty Associated with the Algorithms, Section D.3.5, Outstanding

We believe that it is necessary to experimentally qualify the adequacy of these uncertainties, specifically those associated with the synthesis of axial power distribution. We will require that confirmatory measurements be performed during startup to demonstrate the adequacy of the axial power synthesis by comparing to in-core measurements and analysis for various power conditions.

(2) Conservatism of the CPCS Response to Dropped Control Element Assemblies, Reference 1, Closed

We require three-dimensional transient power distribution studies be performed to assure that effects of dropped off-center CEAs are conservatively predicted by each of the four CPC channels. Our concerns are the adequacy of delta temperature power basis for rapid transients when ex-core sensors are not available.

(3) I/I Converter Isolation Device, Reference 1, Closed

It is the staff's position that the current-to-current (I/I) converter isolation devices be qualified in accordance with specified criteria, and that the results of the qualification tests be submitted for our review including the test plan, test set-up, test duration and acceptability requirements.

(4) CEAC Separation Criteria at the Output of the Optical Isolator Cards, Section D.4.1.4, Outstanding

We will require that the applicant identify their design basis events for the control element assembly calculator (CEAC) and verify that no credible single event either internal or external to the CEAC will result in loss of function.

(5) Cable Separation, Section D.4.1.2, Outstanding

The applicant identified an area where safety-related control rod drive position sensor cables are run together with nonsafety cable. The applicant will reevaluate this design and advise the staff as to its resolution.

(6) Position Isolation Amplifiers, Reference 1, Closed

It is the staff's position that the isolation amplifiers be qualified in accordance with the specified criteria and that the results of the qualification tests be submitted for our review, including the test plan, test set-up, test procedures and acceptability requirements.

(7) Protected Memory, Reference 1, Closed

The ANO-2 memory protection hardware causes instruction attempting to write into protected memory to be converted into read instructions. No safety credit is allowed for this feature unless failures in the system that result in attempts to write in protected memory are annunciated to the operator. Furthermore, if safety credit is desired, we shall require that a status lamp seal indicate the state of operation.

(8) Time Interval of Periodic Testing, Section D.4.2.1, Closed

(a) The applicant is to develop an acceptable analysis of the CPCS reliability in accordance with the requirements of Section 4.4 of IEEE Standard 279-1971 and Section 4.2 and 4.3(1) and (7) of IEEE Standard 338-1971. This analysis will provide the basis for evaluating the performance data obtained in parts 8b and 8c and for establishing and modifying the periodic test interval after the initial operation period.

(b) Completion of the supplemental qualification testing identified in the staff's July 7, 1976 letter and documentation of the system reliability during this test interval is required.

(c) During the first six months of operation, the periodic test interval should be significantly more frequent than the proposed 30 days. The interval could in part be based on the results of (a) and (b) above. All failures during this period should be carefully recorded, classified and analyzed. At the end of the six-month period, the performance of the CPCS should be analyzed using the model developed in (a) above and the operational reliability assessed. Based on these results, the test interval could then be modified.

(9) System Functional Testing, Section D.4.1.6 and D.4.2.1, Closed

The applicant has not provided definitive and adequate procedures for periodically checking and verifying the functional operation of the CPCS in accordance with the requirements of General Design Criterion 21, "Protection System Reliability and Testability" and the guidelines of Section 4.3 of IEEE Standard 335-1971, "Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems." To verify the functional performance of the CPCS and to insure adequate overlap, the periodic test program should be modified to include procedures for testing each trip function in each channel from sensor input to the CPCS to trip output to the reactor trip system. The procedures should be sufficient to verify that the protective action for each function will ensue for the expected extremes for each sensor.

(10) Periodic Testing, Addressable Constants, Section D.4.2.1, Closed

For any changes to addressable constants, the test program will identify calculation errors which may or may not be actual errors. We will require that the applicant develop practical techniques and procedures for verifying calculated results after changes to addressable constants.

(11) Environmental Performance Qualification, Section D.4.2.4, Closed

In accordance with the requirements of IEEE Standard 279-1971, Sections 4.1, 4.3, and 4.4, and IEEE Standard 323-1971, Section 4.3, prior to initial operation, a satisfactory environmental test of the integrated system (exclusive of sensors) should be performed or an acceptable analysis clearly establishing the adequacy of component testing is required for staff evaluation. The staff's July 7, 1976 letter includes the requirements for this qualification testing.

(12) Electrical Noise and Isolation Qualification, Section D.4.4.4, Outstanding

Tests for electrical isolation separation and noise susceptibility will be required. The applicant shall develop and submit for approval test plans and detailed procedures for these tests prior to their undertaking. In addition, due to the CPCS design and packaging, these tests should be performed on the fully configured integrated system or an acceptable analysis clearly establishing the adequacy of component testing is required for staff evaluation. The staff's July 7, 1976 letter provides supplemental details on this concern.

(13) Sensor Qualification, Section D.4.2.4, Closed

For those unique sensors (reactor coolant pump speed and control element assembly position) the applicant is required to submit documentaton to verify their environmental performance qualification.

(14) Seismic Qualifications, Section D.4.2.4, Outstanding

The staff has found the seismic qualification test plan not acceptable. Current criteria for multi-frequency input and sine beat tests for seismic qualification have been provided to the applicant. Submittal date for a satisfactory seismic qualification plan and review completion date have yet to be determined.

(15) Addressable Constants, Section D.3.11, Outstanding

Any changes in addressable constants must be provided with adequate safeguards to protect against unreasonable entries. The proposed safeguards against unreasonable entries are basically administrative and are subject to human error. To enhance safety by minimizing human error and to utilize capabilities of the computer to audit the input, the staff requires that the computer program be modified to conduct reasonability tests and to reject unreasonable values of addressable constants as they are entered from the Operator's Module. The operator is to be notified upon failure of the reasonability test. Qualification testing of the modification must also be conducted.

(16) Quality Assurance Plan, Section D.4.3.4, Closed

The results from our recent audits of the hardware and the software have served to focus our concerns upon the quality assurance program used for system development. Upon evaluation of these results, we have concluded that the applicant is not complying to the quality assurance plan with regard to the following 10 CFR Part 50 criteria:

- (a) Criterion 1, Quality Standards and Records, Appendix A - General Design Criteria for Nuclear Reactor Plants, and

(b) Appendix B - Quality Assurance Criteria for Nuclear Power Plants and Reprocessing Plants.

The bases for this conclusion are deviations from stated positions, the lack of documented system software development guidelines, and design errors uncovered in our review to date.

As stated in Appendix B of 10 CFR Part 50, the Quality Assurance Program must be applied to the design, fabrication, construction and testing of the structures, systems, and components of the facility. It is our position that a Quality Assurance Plan is required for the core protection calculatory system to embrace all activities from the current frozen design (as of November 24, 1975) to the final design of the installed system. An effective quality assurance program is required to minimize design errors and is an important component to the qualitative reliability of the system. The acceptability of the Quality Assurance Plan and the compliance with the plan must be assessed by the staff prior to the completion of the safety evaluation.

In addition to the criteria stated in Appendix B to 10 CFR Part 50, the staff desires to emphasize the positions entitled, "Performance Qualification of Software Change Procedures," with respect to the Quality Assurance Plan.

(17) Performance Qualification Testing, Reference 1, Closed (See Position 24)

For evaluation of dynamic test results, we will require submittal of FORTRAN Codes test results for selected cases to permit comparison with CPCS Performance Qualification test results. In addition, we will require that transient analyses be performed for selected dynamic test cases using the codes normally employed by Combustion Engineering for Section 15.0 of Final Safety Analysis Report transient analyses. This will enable the staff to determine if the time to trip output on the CPCS based on projected DNBR of 1.3 is reached. The trip signal input to the more sophisticated codes will be the time to trip for respective cases on the CPCS.

The staff will accept for review the Phase II Test results previously obtained on the plant system. However, all software revisions since those tests must be implemented in accordance with qualified change procedures (see "Qualification of Software Change Procedure"), and all Phase II test cases must be repeated on the FORTRAN version of the final program. If final test results are not essentially identical to previous results, a repeat of Phase II test on the plant system configuration will be required.

(18) Burn-In Test, Section D.4.4.5, Outstanding

We find the proposed duration of the burn-in test (three to six months) acceptable subject to our review of test ground rules and acceptance criteria

which must be submitted in the form of the test plan before the test commences. We will require that the software on the system during the test incorporate all design changes which have been identified by the applicant and the staff prior to a new freeze on the design. The staff will require testing of the total system after installation of the CPCS and associated process instrumentation in the plant protection system cabinet number 2C15. Failure to incorporate this equipment for the burn-in test will necessitate a more extensive field test program for the entire system.

The staff has reviewed the applicant's supplemental response to position 18, which deals with the Burn-In Test. Based on the new information presented and the additional testing proposed, the execution of the Burn-In Test with the frozen software is acceptable, subject to the conditions stated herein.

Conditions for Hardware Burn-In Test

- (a) A staff review of the test procedures to be used in the hardware Burn-In Test is in progress. These procedures must be consistent with industrial practice for computer system testing and acceptable to the staff.
- (b) Additional tests to demonstrate and evaluate the integrity of software and the integrated system are needed. The staff requires a minimum test period of two weeks, with the system operating continuously on live input signals in addition to satisfactory performance of static and dynamic test cases to demonstrate the integrity of the integrated system. This test must be conducted with the same configuration and the same environment as that used for the hardware burn-in test conducted with the frozen software. This is required to assure that problems encountered after installation of the system in a new environment (the ANO-2 site) do not interfere with evaluation of the final software.

(19) Qualification of Software Change Procedures, Section D.4.4.6, Outstanding

Following are the primary requirements for qualification of software change procedures:

- (a) All changes are to be performed strictly in accordance with the documented quality assurance procedures which are to be available for review by the staff. The documentation must accurately reflect the status of the altered program.
- (b) The FORTRAN version of the modified program is to be subjected to a complete static and dynamic test program to demonstrate conservatism with respect to trip requirements defined by the ANO-2 accident analysis.

- (c) The assembly language version of the qualified FORTRAN is to be subjected to a static and dynamic test program on an acceptable test system. The test program is to include sufficient reactor simulated transient test cases, static test cases and single parameter transient test cases to demonstrate that the program response corresponds to its FORTRAN version. The test program is also to include testing of the man-machine interface.
- (d) The software is to be transferred to the plant system in accordance with the applicant's proposed procedures prior to the burn-in test. All four channels will again be subjected to static and dynamic test cases to demonstrate that the response is identical to that observed on the test bed system. This step is to demonstrate the adequacy of the quality assurance procedures for transfer from the test bed to the plant system.
- (e) Step d need not be repeated for future software revisions. All software design changes and revisions to constants in memory (except addressable constant) are subject to documentation, review and approval by the Regulatory Staff.

(20) Data Link to Plant Computer, Section D.4.2.3, Outstanding

The core protection calculator system is designed with a data link and a special program module in each protection computer to service the plant computer. These data links and programs are an addition to the traditional plant computer interconnects in analog, hard-wired protection system which are also included in the ANO-2 reactor protection system. It is our position that these data links and the plant computer service program do not satisfy the requirements of General Design Criterion 24, "Separation of Protection and Control Systems," and IEEE Standard 279-1971, Section 4.7, "Control and Protection System Interaction," regarding independence of protection systems. Therefore, we will require that the plant computer service data links to the protection computers be removed and that the plant computer service routine be deleted from automatic program scheduling.

(21) Check-sum, Section D.4.2.1, Closed

Our review of the paper tape memory dump representing the frozen design revealed that the check-sum values are not the same in all redundant channels. For consistency and inspection purposes, we require that a procedure be implemented that will result in check-sum agreement between corresponding blocks of all redundant computer channels in the system. Furthermore, the checksums in each channel must be available for inspection purposes through the Operator's Module.

(22) Timeout Error Detection for Penalty Factor Transmission, Section D.4.2.1, Closed

We have noted that the write instruction designed to transmit the penalty factor from each CEAC to each of the CPCs does not have an error response routine for Input/Output (I/O) timeout. Since all other I/O operations in the system have this feature, we shall require that the CEAC-penalty factor write commands be likewise provided with error test and response routines.

(23) Watchdog Timer, Section D.4.1.3, Closed

(a) Core Protection Calculator (CPC)

We shall require an automatic (hard-wired) trip of the associated protection channel upon timeout of the watchdog timer. From the safety review of the design information submitted to date, we have concluded that a significantly larger number of the CPCs safety functions would be monitored if the watchdog timer reset command were moved from the clock interrupt handler to the trip sequence program. In the interest of safety we require that the watchdog timer be reset from this trip sequence program.

(b) Control Element Assembly Calculator (CEAC)

Upon timeout of the watchdog timer, we require that the "fail bit" be set in the CEAC output. From the safety review of the design information submitted to date, we have concluded that a significantly larger number of the CEACs safety functions would be monitored if the watchdog timer reset command were moved from the clock interrupt handler to the penalty factor algorithm module. In the interest of safety we require that the watchdog timer be reset from the penalty factor algorithm module.

(24) Phase II Test and Test Report, Section D.4.4.4, Closed

Upon review of the Combustion Engineering Topical Report CENPD-222 "Core Protection Calculator System (CPCS) Phase II Design Qualification Test Report," we have concluded that the computer program has not been tested to quality standards commensurate with the importance of the safety functions to be performed. On this basis, we find the Phase II Test Report unacceptable, including the test procedures and acceptance criteria utilized for the tests. Furthermore, the test report is incomplete in the analysis of test cases. This has raised concerns about the functional adequacy of the system. Because of these deficiencies, we do not consider the Phase II Test Report as an acceptable verification of the CPCS computer program.

Our major areas of concern are as follows: (Sequence is of no significance all concerns are of equal importance).

- (a) Of the 36 static test cases, 18 failed the stated acceptance criteria. Coding error was the prime cause of not satisfying criteria for 14 cases. For verification purposes, the coding error was deliberately inserted into the FORTRAN simulation program to generate erroneous simulation results to compare with the results produced by the Core Protection Calculator System (CPCS). These procedures are unacceptable. Also, these actions are in direct violation of the stated test procedures described in Section 7A.4.7.6, "Design and Performance Qualification Testing" of the Final Safety Analysis Report.

From the test report, it appears that the coding errors of a fixed point multiplication overflow and a floating point multiplication underflow were detected in the execution of the static test cases and of the dynamic test cases. The execution of test cases with known coding errors in the computer program violates the test procedures stated in Section 7A.4.7.6 of the Final Safety Analysis Report.

Thus, because of the procedures used in the execution of the Phase II test cases (both static and dynamic test cases), we find the test results unacceptable. Also because of the large error tolerances used for evaluating acceptability of test results, we conclude that the verification of the correct implementation of the CPCS protection algorithms is not shown in the test report.

We shall require that the verification of the correct implementation of the protection algorithms be conducted with procedures which as a minimum are described in Section 7A.4.7.6 of the Final Safety Analysis Report. In addition, acceptance criteria must be specified and justified.

- (b) As a result of the analysis of the test cases, several computer program changes have been proposed and are identified in the test report. In general, the test report does not provide the basis of change, such as test case results with explanations of why the change is required. In order to conduct an independent review of the proposed changes, the staff requires the basis for all proposed changes to the program. This must include all changes identified in the test report along with supporting test cases and explanations such as the results for and explanation of dynamic test cases 11 and 21.
- (c) In the discussion on dynamic test acceptance criteria, it is assumed that the initial steady-state deviations may be applied as a uniform bias throughout the transient. An analysis to support this assumption will be required.

- (d) In the discussion of dynamic test case 15, the eight-second delay in trip time is attributed to improper initial conditions of the test case. For this dynamic test case, it is not clear that the delay in trip is uniquely attributable to initial offset in parameters. We shall require that the applicant provide the detailed information to support this conclusion.
- (e) The analysis of the selected dynamic test cases presented in the report are incomplete. Trip time data for each channel and the FORTRAN simulation trip time are presented, but the response comparisons are only conducted for the trip point. No quantitative evaluation of error and error time history between the state variables presented for the FORTRAN simulation and the corresponding CPCS state variables is made. The lack of this comparison does not allow for an assessment of the implementation adequacy of the dynamic algorithms. We shall require that a comparison of the response of principle state variables from the FORTRAN simulation be made with the corresponding state variables of the CPCS. The resulting error history should be sufficiently small (and acceptable to the staff) to demonstrate adequate implementation of the dynamic algorithms. Furthermore, a summary table of trip times for all of the dynamic test cases is required for review purposes.
- (f) The excore detector readings presented in the description do not appear to include sufficient variation in relative magnitude to test all of the various correction options inherent in the local power density trip functional program. We require documentation to clearly demonstrate that the shape correction routines were all correctly implemented and tested.
- (g) In evaluating the static test cases, the staff had difficulty in assessing test procedures, the input parameters used in the test cases and the analysis of the limited number of intermediate and output parameters presented for the testing. In evaluating the input data that were used in the static test cases, we found that the input had been modified for greater than 50 percent of the cases.

To evaluate the above problems, the applicant's test plan must be provided on which the Phase II test report is based. The test plan should include acceptance criteria, the procedures used in the testing, a description of and objectives of each test case, the input data to be used in each case, and especially the parameters and variables to be recorded and analyzed for each test case.

- (h) The Phase II test report does not address a test observed by the staff during which a channel failed to trip. (Trip Report - Demonstration of CPC Testing - November 24-26, 1975). We shall require an analysis of this case as part of the test program.

- (i) **Static Test Acceptance Criteria:** The error bands specified for static test acceptance criteria must be clarified and justified. The clarification should include identification and qualification of error components comprising the overall uncertainty band, the description of how they are combined to obtain the overall uncertainty tolerance. All CPC error components inherent in the Phase II test configuration must be included in the analysis; i.e., analog to digital conversion error, simulator errors, noise effects, and processing error in the digital computation must be quantified and justified in supporting documentation.

Support data must be provided to justify the increase in acceptance criteria (+ five percent error) due to the Power Utility Plant Simulator (PUPS) output hardware, cabling, and noise effects.

- (j) **Dynamic Test Acceptance Criteria:** The previous position of the staff on "Performance Qualification Testing" requires that transient analysis be performed for selected dynamic test cases using the codes normally employed for Section 15.0 of Final Safety Analysis Report transient analyses.

The required time of trip to prevent DNBR from going below 1.3 as determined by these analyses should be specified for applicable cases as one of the acceptance criteria.

- (k) **Scaling Errors:** The staff will require evidence that steps have been taken to preclude additional errors in the scaled range of program variables such as occurred for Static Test Case 14.

- (l) **Round Off Errors:** The staff will require further analysis of the Static Test Case 11 error. It is not clear why the results should be sensitive to an exact equality of two different instrument signals, since the inherent measurement error makes such a comparison meaningless. Discuss provisions which are being taken to assure that other errors of similar logic origin do not exist. The logic should be justified and the deviation in results due to this logic should be quantified.

- (m) **Auto Restarts:** The effect of recurring auto restarts that occurred during the use of test procedures C and D should be discussed. The staff will require details of the program changes designed to resolve this problem. The staff will also require details of the testing planned to conclusively demonstrate that the problem is resolved.

- (n) **Dynamic Test Cases:** A repetition of the dynamic tests will be required. The dynamic test cases are the primary basis for evaluation of the dynamic algorithms. The staff regards that it is necessary to demonstrate the qualification of the corrected design as identified by position 18 (Burn-In

Test). All design changes as identified by the applicant and the staff cannot be adequately evaluated without this testing.

(25) Maintainability of the Core Protection Calculator System, Section D.4.2.2, Closed

IEEE Standard 279-1971, Section 4.21, "System Repair," identifies maintainability as one of the requirements for the reactor protection system. The discussions in Sections 7A.4.8.2.1 and 7A.4.7.2.3 of the ANO-2 Final Safety Analysis Report do not adequately address the maintainability of the Core Protection Calculator System (CPCS). Industrial experience with process computer systems had identified several concerns regarding maintainability of digital computer systems over the operating life of the plant. These concerns are summarized as follows:

- (a) Lack of standardization in hardware and software design has led to difficulties in identifying second sources of parts supply.
- (b) The short commercial life cycle of electronic parts compared to plant operating life has resulted in obsolescence of equipment and unavailability of spare parts.
- (c) Suppliers' and users' lack of experience, trained technicians to maintain equipment.
- (d) Incomplete maintenance and trouble shooting procedures and system documentation has made maintenance difficult.

As a result of these concerns, and since the ANO-2 represents the first system of its type for use in a reactor protection system, we require that the CPCS maintainability plan for the life of the plant be documented and docketed for the regulatory staff's review and evaluation. In addition to the information presented in the Final Safety Analysis Report, the plan should address the following:

- (a) The maintenance actions (i.e., preparation, failure verification and fault location, replacement part procurement, repair and verification tests) required.
- (b) The maintenance diagnostic and repair features (e.g., displays and controls, external accessibility, test points, cables and connectors, internal accessibility, manuals and test equipment).
- (c) Hardware and software maintenance support to be provided by vendors (and/or others) and personnel qualification and training to support this maintenance service.

- (d) Hardware and software maintenance to be provided to the applicant and personnel qualification and training to support this maintenance.

(26) Optical Isolator, Section D.4.1.4, Outstanding

It is the staff's position that as the optical isolator is to be utilized as an electrical isolation device, the applicant must demonstrate that any single credible fault (125 volts alternating current or 125 volts direct current) applied to the device output will not degrade the operation of the circuit connected to the device input. Also, the application of the same credible fault must be applied to the input of the device with no degradation of the circuit connected to the device output. (See Figure 7A.4-23 of the Final Safety Analysis Report).

(27) Periodic Testing of Isolation Devices, Section D.4.2.1, Closed

The unique design of the CPCS relies on many isolation devices (i.e., optical isolators for control element assembly calculator to core protection calculator data transfer and control element assembly position signals) to maintain electrical independence among the protection channels. The ability of these devices to maintain the isolation among channels is one of the bases for accepting the design of the CPCS. It is our concern that failures of the isolation characteristics of these devices would seriously compromise the ability of the CPCS to function. The current periodic test procedures do not include provision for verifying that the isolation characteristics of these devices has not failed. Therefore, it is our position that periodic tests to verify the isolation characteristics of those isolation devices used to ensure channel independence should be performed. We will require that the applicant submit, for our review and approval, a test procedure for periodically checking the isolation characteristics.

TABLE D.2
CPCS REFERENCES AND MEETING MINUTES

REFERENCES

- (1) NUREG-0308, "Safety Evaluation Report, Arkansas Nuclear One - Unit 2, "Docket No. 50-368, U.S. Nuclear Regulatory Commission, November 1977.
- (2) Letter from J. F. Stolz, NRC to W. Cavanaugh, AP&LCo, "Core Protection Calculation System," dated January 18, 1978.
- (3) CEN-44 (A)-P, "Core Protection Calculator Functional Description," January 7, 1977, ANO-2 Unit One. Supplement - 1(P), May 16, 1977, Supplement - 2(P), May 19, 1977, Supplement - 3(P), September 2, 1977.
- (4) CEN-45 (A)-P, "Control Element Assembly Calculator Functional Description," January 7, 1977, ANO-2 Unit One.
- (5) CEN-53 (A)-P, "CPC and CEAC Data Base Document," May 20, 1977, ANO-2, Unit One. Supplement - 1(P), June 28, 1977, Supplement - 2(P), September 2, 1977.
- (6) CEN-63 (A), "CPC/CEAC Startup Test Requirements for ANO-2," July 28, 1977.
- (7) CENPD-145, "INCA - Method of Analyzing In-Core Detector Data," April 1975.
- (8) CENPD-153, "Evaluation of Uncertainty in FQ Measured by Self-Powered Fixed In-Core Detector Systems," August 1974.
- (9) CENPD-170-P and CENPD-170, "CPC Assessment of the Accuracy of PWR Safety System Actuation as Performed by the Core Protection Calculators," July 1975.
- (10) CENPD-170, Supplement 1P and Supplement 1, "CPC Assessment of the Accuracy of PWR Safety System Actuation as Performed by the Core Protection Calculators," November 1975.
- (11) Memorandum for J. F. Stolz, NRC, from G. W. Reinmuth, NRC, Subject: "Inspection of Core Protection Calculator System Design (CPCS) (Arkansas Nuclear One - Unit 2)," December 1977. Enclosures: (1) letter to Combustion Engineering, dated 12/2/77, (2) Inspection Report No. 99900401/77-04.
- (12) CEN-67(A)-P, "Core Protection Calculator System Program Assembly Listing," July 29, 1977.
- (13) CEN-57(A)-P, "Core Protection Calculator Software Specification," June 27, 1977.
- (14) CEN-58(A)-P, "Control Element Assembly (CEAC) Software Specification," July 28, 1977.

- (15) CEN-68(A)-P, "Core Protection Calculator System, Phase II Test Audit," August 8 and 9, 1977.
- (16) CEN-65(A)-P, "Core Protection Calculator System, Phase I Test Audit," July 28 and 29, 1977.
- (17) CEN-55(A)-P, "Phase II Design Qualification Test Procedure," June 24, 1977; Supplement 1-P, July 18, 1977.
- (18) CEN-73(A)-P, "Core Protection Calculator, Phase II Test Report," October 27, 1977.
- (19) CEN-72(A)-P, "Core Protection Calculator System, Phase I Test Report," October 14, 1977.
- (20) CEN-71(A)-P, "Core Protection Calculator, Single Channel Qualification Test Report," October 19, 1977.
- (21) "EMI Test Procedure for the Core Protection Calculator System," February 16, 1977.
- (22) CEN-52(A), "EMI Test Report for the Core Protection Calculator," May 11, 1977.
- (23) Letter to J. F. Stolz, NRC, from D. A. Rueter, Arkansas Power and Light Company, "CEA Calculator Separation Criteria," September 22, 1976.
- (24) CEN-70(A), "Test Procedure for the CPC Data Link Fault Isolation," August 12, 1977.
- (25) CEN-74(A), "Isolation Test Report for the Core Protection Calculator System," November 14, 1977.
- (26) Letter to J. F. Stolz, NRC, from D. A. Rueter, Arkansas Power and Light Company, "CPC Position Responses," June 13, 1977, 2-067-3.
- (27) Letter from Arkansas Power and Light Company to J. F. Stolz, March 14, 1977, "CPCs: RSPT Irradiation," and letter, Combustion Engineering, F. C. Sernatinger to C. B. Brinkman, August 5, 1977.
- (28) "Test Report for Thermal Test of the Process Protective Cabinet," January 1978.
- (29) "Environmental Qualification Test Report for the 150" Reed Switch Position Transmitter and Bendix Electrical Connector," October 29, 1976.
- (30) "Environmental Qualification Test Report for the Reactor Coolant Pump Shaft Speed Sensor System," September 30, 1976.

- (31) Letter 2-037-7, Arkansas Power and Light Company to J. F. Stolz, NRC, "CPC Staff Position 25," March 14, 1977.
- (32) Letter, A-CE-6283, "CPCS Proposed Resolution of Positions 9, 18, 26, and 27," May 31, 1977.
- (33) "System Qualification Test Procedure for Core Protection Calculator System," September 23, 1976, Rev. 0.
- (34) CEN-51(A), "System Qualification Final Test Report for Core Protection Calculator System," May 9, 1977.
- (35) CEN-51(A), Supplement 1(P), "Reliability Prediction Calculation for the Core Protection Calculator System," May 1977.
- (36) CEN-66-P, "Reliability Calculation for the CPCS Sensor Input Module," August 16, 1977.
- (37) CEN-62(A), "Test Procedure for the Periodic Verification of Optical Isolation in the Core Protection Calculator System," July 22, 1977.
- (38) CEN-61(A), "Test Procedures for the Periodic Verification of the Control Element Assemblies Position Isolation Assembly Isolation Properties," September 28, 1977.
- (39) CEN-61(A), "Test Procedures for the Periodic Verification of the Control Element Assemblies Position Isolation Assembly Isolation Properties," Rev. 01, January 1978.
- (40) Letter from Arkansas Power and Light to J. F. Stolz, "Proposed Resolution to Position 10," June 13, 1977.
- (41) Letter to William Cavanaugh, Arkansas Power and Light, from J. F. Stolz, NRC, "Core Protection Calculator System Pre-Operational Test (Arkansas Nuclear One - Unit 2)," dated December 9, 1977.
- (42) CEN-64(A)-P, "CPCS - Core Flow Stability Assessment," August 1977.
- (43) Letter to William Cavanaugh, Arkansas Power and Light, from J. F. Stolz, NRC, "Requests for Additional Information (Arkansas Nuclear One - Unit 2)," September 7, 1977.
- (44) Letter to L. Beltracchi, NRC, from K. L. Gimmy, E. I. Dupont, Atomic Energy Division, Savannah River Plant, August 25, 1977.
- (45) Letter from J. D. Phillips, Senior Vice President, Arkansas Power and Light Company to Director of Nuclear Reactor Regulation, U.S. Nuclear Regulatory Commission, "CPC Position 20," July 7, 1977.

(46),

- (47) Letter from J. D. Phillips, Senior Vice President, Arkansas Power and Light Company to Director of Nuclear Reactor Regulation, U.S. Nuclear Regulatory Commission, "CPC Position 20," July 29, 1977. Attachment: "Arkansas Nuclear One - Unit 2, Core Protection Calculators, Position 20."
- (48) Letter from D. B. Vassallo, NRC, to M. C. Bender, Advisory Committee on Reactor Safeguards transmitting a Draft Safety Evaluation Report on the CPCS, dated May 2, 1978.
- (49) Letter from S. J. Ditto, Oak Ridge National Laboratory to T. A. Ippolito, Chief, Instrumentation and Controls Branch, USNRC, "Data Links Between Plant Computer and Core Protection Calculators," August 4, 1977.
- (50) Letter from R. S. Boyd, Director, Division of Project Management, ONRR, USNRC to Arkansas Power & Light Company, "Core Protection Calculator Position No. 20," September 20, 1977.
- (51) Letter from William Cavanaugh III, Executive Director of Generation and Construction, Arkansas Power and Light Company to Director Nuclear Reactor Regulation, USNRC, "CPC Position 20," October 25, 1977.
- (52) Letter from R. S. Boyd, Director, Division of Project Management, ONRR, USNRC to Arkansas Power and Light Company, "Core Protection Calculator Position 20," January 19, 1978.
- (53) CENPD-222-P, "Core Protection Calculator System Phase II Design Qualification Test Report," June 1976.
- (54) Letter, Arkansas Power and Light Company, to Director, NRR, "CPCS - Position 24," File 2-1510, January 10, 1978.
- (55) Letter from J. F. Stolz, NRC, to W. Cavanaugh, Arkansas Power and Light Company, "Request for Additional Information on CPCS," dated September 16, 1977.
- (56) CEN-60(A), "Core Protection Calculator Integrated System Burn-In Test Procedure," issued November 18, 1977.
- (57) CEN-60(A) Supplement 1, "Core Protection Calculator Integrated System Burn-In Test Procedure," issued October 4, 1977.
- (58) CEN-69(A)-P, "Core Protection Calculator System, CPC/CEAC Executive System Software Specification," July 27, 1977.

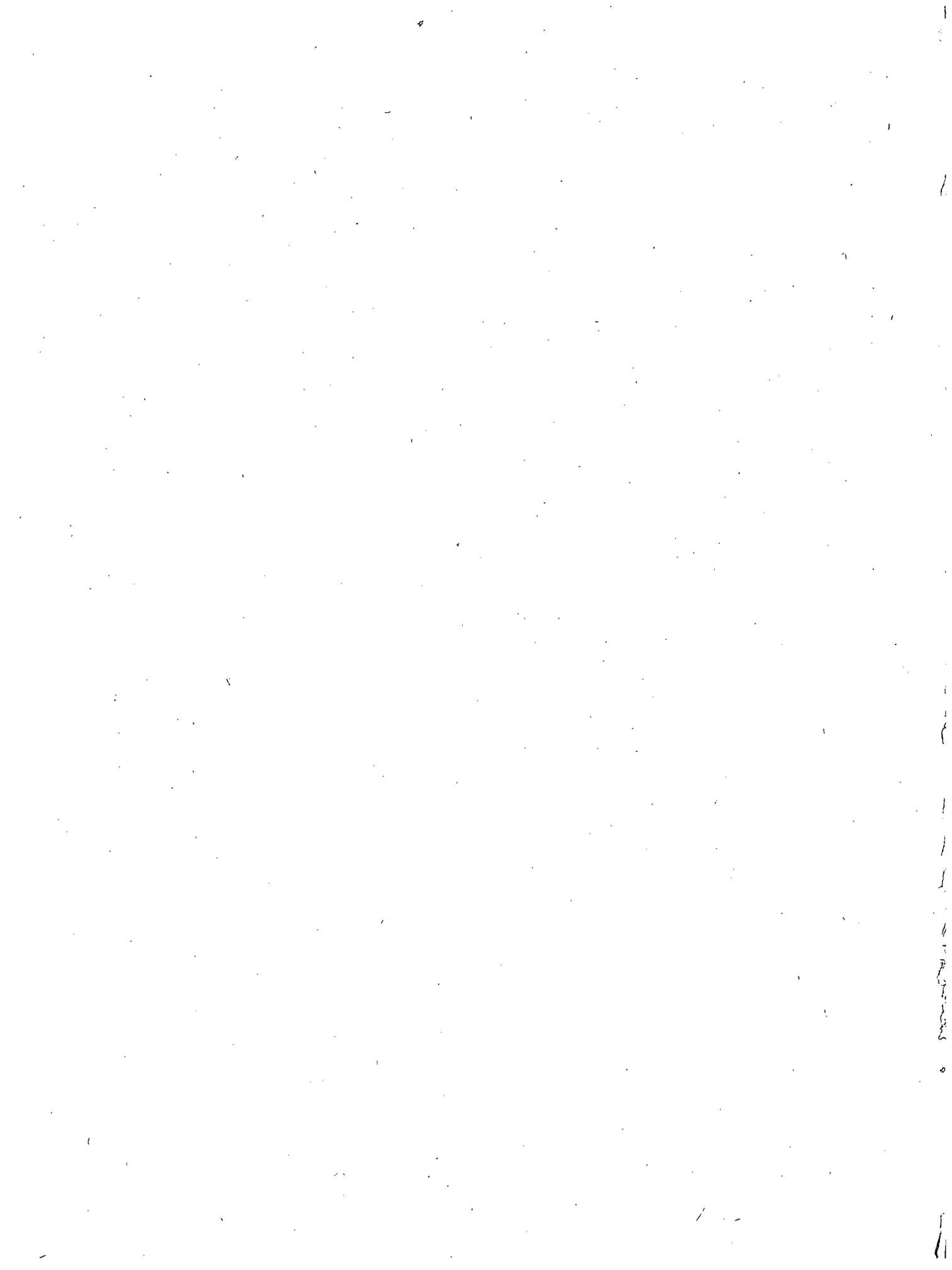
MINUTES OF MEETINGS

The following meeting minutes reflect meetings and audits conducted during the period of February 1977 to early January 1978, with previous activity reported in the Safety Evaluation Report.

- M15 "Trip Report of February 10-11, 1977 - Staff audit of the Core Protection Calculator System (CPCS) Hardware Burn-In Test," dated May 12, 1977, to T. A. Ippolito, Division of Systems Safety, NRC.
- M16 "Trip Report, June 14, 1977, Staff Audit of Functional Descriptions and Data Base Documents," dated August 8, 1977, to T. A. Ippolito, Division of Systems Safety, NRC.
- M17 "Trip Report - Phase I Test Audit - Core Protection Calculator System," dated August 26, 1977, to T. A. Ippolito, NRC.
- M18 "Trip Report - Phase II Test Audit, Software Burn-In Test Audit - Core Protection System," dated September 20, 1977, to T. A. Ippolito, NRC.
- M19 "Trip Report - Core Protection Calculator System (CPCS) Process Protective Cabinet Thermal Tests - September 27-29, 1977," dated October 12, 1977 to T. A. Ippolito, NRC.
- M20 "Meeting Minutes - Core Protection Calculator Systems - October 28, 1977," dated November 14, 1977, to T. A. Ippolito, NRC.
- M21 "Trip Report - Assessment of Test Reports - Core Protection Calculator System," dated December 20, 1977, to T. A. Ippolito, NRC.
- M22 "Trip Report - Core Protection Calculator System (CPCS) Discussion of Positions 5, 8, 9, 12, 23, 26 and 27 and Audit of Optical Isolator Qualification Tests - October 7, 1977 to T. A. Ippolito, January 6, 1978.
- M23 "Trip Report - Core Protection Calculator System (CPCS) EMI Noise Immunity Tests - March 31, 1977," to T. A. Ippolito, April 8, 1977.
- M24 "Summary of Meeting with Arkansas Power and Light and Combustion Engineering, June 1, 1977," to T. A. Ippolito, June 21, 1977.







1943

0 0

1943

1943

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

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, \$300

POSTAGE AND FEES PAID
U.S. NUCLEAR REGULATORY
COMMISSION

