

SAFETY EVALUATION
BY THE PLANT SYSTEMS BRANCH
EMERGENCY CORE COOLING SYSTEM
REVIEW
ARKANSAS NUCLEAR ONE, UNIT 1 (ANO-1)
DOCKET NO. 50-313

I. INTRODUCTION

The Arkansas Power and Light Company, pursuant to the Commission's order for modification of license dated December 27, 1974; submitted a re-evaluation of Emergency Core Cooling System (ECCS) cooling performance that conforms with the requirements of Appendix K 10 CFR Part 50, in its letter of July 9, 1975. The licensee in response to the staff's request for additional information^{1/} and later staff queries into specific areas submitted data necessary to permit completion of an evaluation of the electrical and instrumentation subsystems of ECCS against the single failure criterion in its submittals listed in the reference section of this report. This Safety Evaluation Report discusses the review of the aforementioned ANO-1 documentation submitted by the Arkansas Power and Light Company

However, Arkansas Power and Light Company (AP&L) in its reportable occurrence No. 50-313/77-19 of September 20, 1977 described how a design review for ANO-2 had revealed an oversight in the design of emergency ventilation in several vital equipment areas in the ANO-1 plant. The corrective actions the licensee proposed to resolve the concerns associated with the design oversight were presented in a program which consists of three phases. The first and immediate phase was to provide temporary emergency ventilation for the electrical equipment areas and was reviewed and reported in the staff's safety evaluation of October 24, 1977. In its letter of December 21, 1977, the licensee submitted its proposed design for the interim installation, which is to remain in effect until 1979. The interim installation, the second phase of the program, was reviewed and reported in the staff's safety evaluation of August 9, 1978. The staff is presently in the process of reviewing the final design of permanent measures which will be reported in a separate safety evaluation. Also the degraded voltage analysis for this plant as well as any issues which have grown from the Three Mile accident will be reported by the staff under separate safety evaluations.

II. EVALUATION

We have performed an evaluation of the Arkansas Nuclear One, Unit 1 Plant ECCS in the following specific areas:

^{1/}"Generic information request for review of ECCS in the Electrical Instrumentation and Control Areas," dated May 7, 1976.

967 181

7909190 368

1. Emergency Core Cooling System Actuation System
2. Onsite Emergency Power System
3. Electrical Equipment Qualifications
4. Submerged Electrical Equipment
5. Electrically Operated Fluid System Components
6. Single Failure Criterion
7. Electrical Interlocks
8. Electrical and Physical Separation Criteria
- A. Emergency Core Cooling System Actuation System

The Emergency Core Cooling System (ECCS) actuation system is part of the Engineered Safety Features Actuation System (ESFAS) which is a protection system that initiates operation of various engineered safety features equipment to mitigate the consequences of a loss-of-coolant accident. The ESFAS monitors two variables, low reactor coolant pressure and high reactor building pressure, to detect loss of reactor coolant system or the secondary system (inside containment) boundary integrity. The ESFAS is two-out-of-three coincidence logic system. The system is comprised of three redundant and independent analog subsystems. The analog subsystems supply two redundant and independent digital subsystems, each capable of initiating the required Engineered Safety Features (ESF) through five actuation groups. The emergency core cooling portion of the ESF actuated by the (ESFAS) consists of High Pressure Injection (HPI) and Low Pressure Injection (LPI) systems.

Topical Report, BAW-10003 "Qualification Testing of Protection System Instrumentation" (Rev. 4, January 1976) contains the single failure analysis of Babcock & Wilcox's (B&W) Engineered Safety Features Actuation System (ESFAS) used to initiate all ECCS. Although the ANO-1 ESFAS equipment was required to be designed to IEEE-279-1968 rather than IEEE-279-1971, BAW-10003 has been generically accepted by the NRC (Ltr. A. Schwencer to K. E. Suhrke dated October 10, 1975), for plants required to meet both the 1968 and 1971 versions of IEEE-279. It should be noted that, with respect to single failures, the 1968 and 1971 versions of IEEE-279 differ only in treatment of protection-control interfaces, and ESFAS has no such interfaces. Therefore, the statement of single failure requirements applicable to ANO-1 is identical in both IEEE-279-1968 and IEEE-279-1971 and no changes are proposed for the ANO-1 ESFAS.

Based upon a review of the information the licensee has provided and of the previous evaluation of this system at the operating license review stage, we have determined that the original design meets the single failure criterion and present staff requirements; and, therefore, is acceptable.

967 182

B. Onsite Emergency Power System

The onsite emergency power system supplies electrical power to the engineered safety features equipment whenever there is a partial or a total loss of offsite power, and is comprised of two redundant and independent distribution systems. Each distribution system includes 4160, 480, and 120 volt (a.c.) load centers powered by a 4160 volt, 2600 kw diesel generator; a d.c. distribution center powered by a 125 volt battery and battery bank charger unit (a third charger can serve either d.c. bus); and two inverters.

The ECCS safety loads are distributed evenly between the two distribution systems with the exception of the third high pressure injection pump and the third service water pump. These pumps can be powered from either Train A3 or Train A4 distribution system through separate breakers. The selection of the power feed will be accomplished manually through interlock bus-transfer switches which prevent interconnection of the power supplies. In addition, there is a single 480V motor control center which can be manually connected to either one of the distribution systems through a mechanically interlocked transfer switch. The discussion of the review of these interlocks is contained in Section F below. The onsite electrical power distribution system satisfy the recommendations of Regulatory Guide 1.6, "Independence Between Redundant Standby (Onsite) Power Sources and Between Their Distribution Systems."

Each distribution system is capable of furnishing power to equipment load groups which meet the minimum requirements to safely shutdown the reactor. Furthermore, each system is capable of providing sufficient electrical power to all functions necessary to operate the systems which mitigate the consequences of a loss-of-coolant accident.

C. Electrical Equipment Qualification

The qualification requirements for safety-related equipment are a measure of the equipment's ability to withstand the design basis environmental and seismic conditions.

The licensee documented with the exception of radiation that all safety related motors, cables, instruments and other equipment located inside the containment which must operate during and subsequent to an accident, will be capable of function under the following post accident conditions: temperature 286°F, pressure 59 psig, and humidity 100%. An environmental and seismic qualification program was implemented by B&W, the NSSS manufacturer, for confirming that all safety related instrumentation located in the containment would satisfy the above listed LOCA conditions. This qualification program (B&W topical report BAW-10003 "Qualification Testing of Protection System Instrumentation") has demonstrated by testing the operability of the instrumentation and electrical equipment under LOCA conditions inside containment. The level of radiation to which the instrument were exposed in BAW-10003 was 2×10^4 roentgens. This level of radiation exposure satisfied the criteria then current for the period

967 183

of construction phase of this plant. However, this level of radiation exposure is presently being evaluated under the review of IEB 79-01. Until this issue is resolved, it will remain as an "open" issue which will be reported in a subsequent safety evaluation. On the basis of documentation and acceptance by the staff of Topical Report BAW-10003, we have concluded with the exception of the "open" issue that the equipment located inside the containment is environmentally qualified.

The licensee has documented in the FSAR that the seismic testing program meets the requirements of IEEE Standard 344-1971, "Seismic Qualification of Class I Electric Equipment for Nuclear Power Generating Stations." The seismic qualification program under B&W 10003 confirmed that all seismic Category I instrumentation and electrical equipment will operate properly during an SSE and post-accident conditions. This qualification program has demonstrated by testing the operability of the instrumentation and electrical equipment under SEE conditions. On the basis of documentation in the FSAR and acceptance by the Staff of Topical Report BAW-10003, we have concluded that the seismic design of this equipment is acceptable.

D. Submerged Electrical Equipment

The licensee's analysis has shown that the maximum depth of water which can accumulate in the primary containment building following a LOCA will be 8'-9". This yields an upper elevation of water in the containment of 345'-3" (bottom of the containment building is elevation 336'-6"). No other motor-operated valves are located between elevation 345'-3" and elevation 357'-0", thus a very conservative depth of water of 20.5 feet may be considered.

The licensee has surveyed the primary containment building, and all the electrical equipment which is located below the LOCA flood level (elevation 345'-3") has been identified and is discussed below:

1. Submerged Motor-Operated Valves Required for ECCS

The licensee has listed in submittals dated July 9, 1975 and August 3, 1976 those motor-operated valves required to operate for short or long term cooling located inside containment that could become submerged following a LOCA. These valves are:

- CV-1050 reactor coolant hot leg loop A to DHRS
- CV-1410 reactor coolant hot leg loop A to DHRS
- CV-1414 reactor building sump to DHRS
- CV-1415 reactor building sump to DHRS

Valves CV-1050 and CV-1410 are normally closed. Following a LOCA, these valves may be required to circulate borated water to prevent boron precipitation. Fully qualified submersible valve operators have been purchased and installed on valves, CV-1050 and CV-1410.

967 184

They are qualified to operate submerged after being exposed to the LOCA environment.

Valves CV-1414 and CV-1415 are normally open. Following a LOCA these valves are required to operate (open and close) for long term ECCS functions. CV-1414 and CV-1415 and their related raceway are fully submersible, and are qualified to operate submerged following a LOCA.

The licensee has documented that the Rotork submersible valve operators for valves CV-1050, CV-1410, CV-1414, and CV-1415 were designed to remain functional in a submerged condition for 30 days with a maximum fluid temperature of 271°F decaying to 130°F in 30 days, and at a maximum pressure of 53 psig decaying to 5 psig in 30 days. Qualification tests for this type operator were done at a maximum pressure of 70 psig and a maximum temperature of 370°F. The valve operator was submerged in a solution of the same chemistry as the reactor building spray for 30 days with no failure. These valves can be depended upon to operate for at least 30 days under post-accident conditions.

We conclude that flooding of motor-operated valves CV-1050, CV-1410, CV-1414 and CV-1415 following a LOCA will not prevent proper operation of the ECCS and are, therefore, acceptable.

2. Submerged Motor-Operated Valves Required for Containment Isolation

The following listed valves which are located below maximum flood evaluation inside containment are not required to operate for short or long term ECCS cooling. However, these valves do receive a containment isolation signal.

CV-1214 (N.O.) steam generator letdown cooler outlet valve
CV-1216 (N.O.) steam generator letdown cooler outlet valve
CV-1053 (N.C.) reactor coolant quench tank (T42) discharge
isolation valve
CV-1054 (N.C.) sampling line (3/4 inch) isolation valve
CV-4446 (N.C.) reactor building sump connection to auxiliary
building sump valve.

In those cases, where the valves are open, they close to isolate the containment. These valves are required to operate immediately upon the occurrence of a LOCA, are environmentally qualified for the LOCA environment, and they perform their functions before any appreciable accumulation of water in the bottom of the containment. An auxiliary relay energized by containment isolation signal blocks the "opening" circuits of the valves and precludes spurious opening of the valves. Consequently, the above listed valves are not required to be qualified for submerged operation.

967 185

Protective measures have been taken to insure that these valves will not cause loss of vital motor control centers because of electrical faulting at the valve drive motors following submergence. The 480 V MCC Combination motor starters are provided with an instantaneous trip element and an overload relay for each phase. This provides penetration, motor and cable protection, and the isolation of individual motor circuit faults so as not to effect other MCC loads. The control circuits associated with the 480 V MCC are protected by control circuit fuses to isolate electrical faults and to limit the effects of such electrical short circuits to the circuit involved. The 120 V ac/125 V dc instrument Protection is similar to the power protective circuits with the exception that fuses are used to protect loads. For a fault, the fuse has a faster clearing time than the breaker above it. Thus, selective tripping is assured. It is documented that the breakers have been and are periodically tested against the calculational curves providing operational assuredness.

We conclude that the above designs as discussed for preventing malfunctions of the emergency power systems resulting from submergence of equipment inside containment are acceptable.

E. Electrically Operated Fluid System Components

The following systems were analyzed in accordance with EICSB Branch Technical Position BTP-18, "Application of the Single Failure Criterion to Manually-Controlled Electrically Operated Valves" to determine if a single failure could result in loss of capability to perform a safety function:

1. Service Water System,
2. Reactor Coolant System
3. Decay Heat Removal System (low pressure injection)
4. Makeup and Purification System (high pressure injection)
5. Reactor Building Spray System
6. Core Flooding System

These systems were first reviewed by the Reactor Safety Branch to determine those manually-controlled electrically-operated valves which were present and required to satisfy single failure by compliance with BTP EICSB-18. Upon determining these valves, an analysis was performed individually to evaluate the potential consequences of these valves failing in an unsafe position. The determination yielded four valves which could potentially have adverse effects on safety system operation if failure occurred. These valves are as follows:

967 186

1. CV2417 core flooding tank vent valve (CF-3A)
2. CV2420 core flooding tank vent valve (CF-3B)
3. CV3823 service water discharge to emergency pond
4. CV3824 service water discharge to flume

The four valves whose improper function could potentially have adverse effects on safety system operation are discussed below under proposed design changes deemed necessary to meet the single failure criterion.

F. Proposed Design Changes to Meet Single Failure Criterion

A spurious actuation of the Core Flooding Tank (CFT) vent valves CV2417 and CV2420 would result in a decrease in CFT pressure. These valves are manually controlled, electrically operated isolation valves. However, each of these valves is equipped with a pressure reducing orifice. This orifice controls the rate at which the CFT pressure decreases. An alarm would occur when the tank depressurized to 585 psig, approximately 15 minutes following valve failure. It has been estimated it would take an additional 15 minutes for the tank to vent below Technical Specification limits (575 psig), allowing more than sufficient time for the valve to be closed manually. Valves CV2417 and CV2420 which are environmentally qualified for LOCA environment, are not accessible during LOCA. However, dual indication of tank pressure is provided in the control room to detect and alarm (visual and audible) any decrease in tank pressure which may occur due to operator error or electrical fault. For these reasons it is deemed no modifications are required. We find this acceptable.

The service water return discharges either to the recirculating water discharge flume through valve CV 3824 (during normal operation) or to the cooling pond through valve CV3823. These two valves are administratively controlled by operating procedures so that only one of the discharge paths is in service at any particular time. The inadvertent closure or the single failure of the return valve (CV3823 or CV3824) will result in the loss of cooling for both low pressure injection (LPI) strings and to all ECCS components and provides no discharge for service water. For this reason during operation, procedures require the circuit breaker for the valve in service to be removed from the circuit and tagged. The valve handwheel is also tagged to prevent inadvertent operation. Inadvertent closure or single failure resulting in the closure of the open service water discharge valve is immediately alarmed in the control room. The alarm is actuated from high differential pressure across service water pumps (2 alarms). Pump discharge pressure (each pump) is indicated in the control room. The service water discharge valve position and service water system flow are also displayed in the control room. This instrumentation allows the operator to evaluate the situation and initiate opening of the alternate discharge path.

967 187

Based on racking out of the discharge valve circuit breaker, the redundant alarms in the control room, and other available instrumentation as described in the above analysis, it is concluded that a single failure or operator error will not result in adverse consequences to ECCS performance; and therefore, is acceptable.

G. Electrical Interlocks

Electrical interlocks are used as a means of preventing redundant safety divisions from being tied together, thus compromising the electrical independence of redundant power divisions.

There are several points in the distribution system which allow for energizing equipment from the redundant power sources. These exist at the various voltage levels: 4160, 480, 120 and 125 (d.c.) and are addressed in the following paragraphs. Interlocks provided at each voltage level satisfy the single failure criterion and the intent of Regulatory Guide 1.6.

1. 4160 Volt Redundant Bus

The two manually operated tie breakers between the two 4160 volt redundant buses are interlocked so that neither breaker can be closed when both emergency buses are supplied from the nonredundant 4160 volt buses (condition during normal operation), or when the two diesel generators are supplying the 4160 volt emergency buses. These interlocks consist of auxiliary contacts on the 4160 volt circuit breakers and interconnecting wiring.

Of the safety loads, a third high pressure injection pump and a third service water pump can be powered from either distribution system through separate breakers. The selection of the power feed will be accomplished manually through interlock bus-transfer switches which prevent interconnection of the power supplies.

2. 480 Volt Load Center Redundant Breakers

The two tie breakers between the redundant load center buses are interlocked so that both breakers cannot be closed when the two redundant load center buses receive power simultaneously through the incoming circuit breakers. These interlocks consist of auxiliary contacts on the 480 volt load center breakers and interconnecting wiring.

967 188

3. 480 Volt Motor Control Center Redundant Buses

The redundant MCC buses have no interconnecting tie breakers, with the exception of one common MCC (B56) which receives power from the load center redundant buses through breakers and a transfer switch. Assurance against interconnection of redundant emergency buses via the common MCC is accomplished by the manually operated transfer switch which can only be in one or the other position enabling power supply from one or the other load center emergency bus.

4. 120 Volt, A.C. Redundant Buses

Power supply to the 120 volt instrument AC distribution panels is accomplished from either motor control center redundant bus. The tie breakers between the two instrument AC distribution panels are normally open and are provided with keyed locks.

5. 125 Volt, D.C. Redundant Buses

The two redundant DC buses, supplied from separate batteries have tie connections through manually operated breakers and transfer switches. The redundant buses cannot be interconnected since the manually operated transfer switch has one contact open when the other contact is closed. In addition to the battery chargers which separately supply the redundant DC buses, there is one common battery charger which can be used to charge either battery, but not both simultaneously. Simultaneous charging is prevented by a manually operated transfer switch which has a mechanical interlock that will open one set of contacts connected to one redundant bus when the set of contacts connected to the other redundant bus is closed.

We have determined that the manual transfer switches installed and the interlocks provided to prevent the propagation of faults to the redundant safety buses are adequate. Therefore, it is concluded that the interlock systems designed to prevent compromising electrical independence are acceptable.

H. Electrical and Physical Separation Criteria

Engineered safety features circuit separation includes separation of power sources, control and power devices, protective devices, sensors and the interconnecting cables.

The engineered safety features 4160 volt switchgear, 480 volt load centers and motor control centers are located within a Category I structure area to minimize exposure to mechanical, fire and water damage.

267 189

Within practical limits, nonsegregated, metal-enclosed 4160 volt buses are used for all major bus runs where large blocks of power are to be carried. The routing of this metal-enclosed bus minimizes its exposure to mechanical, fire and water damage.

The application and routing of control, instrumentation and power cables minimizes their vulnerability to damage from any source. Cables related to engineered safety features systems have color coded identification and have been routed and installed to maintain the integrity of their respective redundant channels.

Cable is carried in raceway systems consisting of rigid and flexible conduit, galvanized steel cable tray, junction boxes, containment penetrations and raceways within equipment cabinets. Power, control and instrument cables are run in separate raceway systems. When power, control and instrument trays occupy the same area, they are arranged vertically with the power trays on top and the control and instrumentation located in the lower trays.

The separation of redundant cables of the engineered safeguards systems circuits is accomplished by spatial separation where cables are installed in trays.

Separation distances for trays containing redundant cables are as follows:

1. Horizontal Separation

In rooms containing heavy rotating machinery or high pressure pipe lines, a minimum separation of 20 feet or a 6" thick reinforced concrete wall is provided. In fire hazare areas a separation of 3 feet or a barrier equivalent to one inch of transite, covered with a sheet of 16 gauge steel is provided.

2. Vertical Separation

A vertical separation of 5 feet is provided. Where physical conditions do not permit 5 feet of separation, either the lower tray is equipped with a solid steel cover or the upper tray is equipped with a solid steel bottom, or a barrier similar to the one described for horizontal separation, has been provided. Engineered safety feature system, and Class IE electrical system components mounted on control boards, panels, and relay racks are uesigned and physical separated by a steel barrier or at least 6 inches of air space. In control panels, some wiring and components are common to the two redundant safety system channels. Also in many cases interlocks are required between equipment of different channels

267 190

to perform certain safety functions. The cables containing these common or interlocking conductors are color coded green when they are routed through the raceway system between panels belonging to different safety channels. These cables are run in flexible steel conduits inside the control panels. The flexible steel conduit is extended as close to the terminals as physically possible.

The Fire Protection review required certain modifications to improve the separation in various areas of the plant where the existing cable separation was found inadequate to assure that fire will not cause damage to redundant safe shutdown equipment. The licensee has proposed rerouting of cables or isolating the associated circuits with relay contacts where subject to being disabled by fire in nonsafety-related circuits associated with safe shutdown systems.

On the basis of our review of the original separation criteria described above and the upgrading of separation accomplished under fire protection review, it is concluded that the physical independence of electrical systems is acceptable.

III. Conclusion

The staff has completed its review of the licensee's ECCS performance single failure analysis and has concluded:

- A. The original design of the emergency core cooling system actuation system meets the single failure criterion and present staff requirements.
- B. The onsite emergency power system meets the single failure criterion.
- C. The safety-related electrical equipment is environmentally and seismically qualified except for the 'bper' issue of level of radiation exposure. This issue will be reported in a subsequent evaluation.
- D. The submergence of equipment inside containment will not prevent the proper operation of the emergency core cooling system, containment isolation systems, nor cause malfunctions of the emergency power systems.
- E. The redundancy of systems and valves satisfy the requirements of EICS Branch technical position 18, and precludes the malfunctioning of the emergency core cooling system due to operator error or single failure of electrically operated fluid system components.

067 191

- F. The interlocks provided to prevent the propagation of electrical faults between redundant safety buses satisfy the requirements of Regulatory Guide 1.6.
- G. The electrical and physical separation between redundant divisions satisfies the separation criteria current for the period of construction of this plant and will not cause functional loss of redundant emergency core cooling system equipment.

It is concluded, in summary, that the emergency core cooling system at ANO-1 satisfies the single failure criterion, is seismically qualified, and is environmentally qualified except for the "open" issue; and therefore, is acceptable.

967 192

REFERENCES

1. Letter from D. Ziemann (AEC) to J. Phillips (AP&L) dated December 27, 1974.
2. Letter from W. Cavanaugh III (AP&L) to A. Giambusso (NRC) dated April 21, 1975.
3. Letter from J. Phillips (AP&L) to A. Giambusso (NRC) dated July 9, 1975.
4. Letter from D. Ziemann (NRC) to J. Phillips (AP&L) dated July 22, 1975.
5. Letter from D. Ziemann (NRC) to J. Phillips (AP&L) dated May 7, 1976.
6. Letter from W. Cavanaugh III (AP&L) to D. Ziemann (NRC) dated August 3, 1976.
7. Letter from D. Rueter (AP&L) to D. Ziemann (NRC) dated August 20, 1976.
8. Letter from D. Williams (AP&L) to D. Davis (NRC) dated November 23, 1977.
9. Letter from D. Williams (AP&L) to D. Davis (NRC) dated January 20, 1978.
10. Letter from R. Reid (NRC) to W. Cavanaugh III (AP&L) dated March 20, 1979.
11. Letter from D. Trimble (AP&L) to R. Reid (NRC) dated June 29, 1979.
12. Letter from D. Trimble (AP&L) to K. Seyfrit (NRC) dated July 13, 1979.

967 193