

ENCLOSURE

U.S. NUCLEAR REGULATORY COMMISSION  
REGION IV

Inspection Report: 50-313/95-24  
50-368/95-24

Licenses: DPR-51  
NPF-6

Licensee: Entergy Operations, Inc.  
1448 S.R. 333  
Russellville, Arkansas

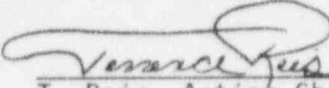
Facility Name: Arkansas Nuclear One, Units 1 and 2

Inspection At: Russellville, Arkansas

Inspection Conducted: August 28 through September 6, 1995

Inspector: J. F. Melfi, Resident Inspector

Approved: \_\_\_\_\_

  
T. Reis, Acting Chief, Project Branch C

10-20-95  
Date

Inspection Summary

Areas Inspected (Unit 1): No inspection of Unit 1 was performed.

Areas Inspected (Unit 2): Special, announced inspection of a licensee identified Unit 2 design deficiency where a single failure of a direct current electrical bus could affect both trains of the emergency feedwater system.

Results (Unit 2):

Operations

- The licensee's Technical Specification (TS) action statement declarations were appropriate to the circumstances (Section 4).
- Operations transferred plant loads from Startup Transformer 3 to the unit auxiliary transformer and back several times during the timeframe in which the single failure vulnerability existed. Transfer from Startup Transformer 3 was performed due to concerns about the potential for a lightning strike affecting Startup Transformer 3. When the threat of lightning subsided, transfer from the unit auxiliary transformer to Startup Transformer 3 occurred in order to exit the TS action statement imposed on the emergency feedwater (EFW) system due to the single failure vulnerability. Although transferring to the UAT constituted

voluntary entry into a TS action statement, given the information available at the time, the action was not inconsistent with conservative facility operation and was not precluded by regulatory requirements (Section 4).

- The licensee's finding and aggressive resolution of the subtle design deficiency through validation of abnormal operating procedures (AOPs) demonstrated operations leadership in addressing plant issues (Section 4).

#### Engineering

- Engineering developed a modification to address the single failure vulnerability in an expeditious manner (Section 4).
- The introduction of the design flaw in 1983 through the modification process is not indicative of current engineering performance (Section 5).

Results (Unit 1): Not Applicable

#### Summary of Inspection Findings:

##### New Items

- One noncited violation (Section 5).

##### Closed Items

- Licensee Event Report (LER) 368/95-001 (Section 6).

##### Attachments:

- Attachment 1 - Persons Contacted and Exit Meeting
- Attachment 2 - Emergency Feedwater Pump and Valve Configuration

## DETAILS

### 1 BACKGROUND

The purpose of this special inspection was to review the circumstances where a single failure of a direct current (dc) vital bus could render both EFW system trains inoperable. This inspection also reviewed subsequent actions taken by the licensee, which included realignment of electrical power sources to preclude this single failure from affecting both EFW trains and, later, changing the alignment several times when there was a concern that lightning in the area threatened stability of the alternate power source configuration.

### 2 SYSTEM DESCRIPTION

The following descriptions are relevant aspects of the EFW system, the vital dc buses, and the 4160 volt-alternating current (Vac) system.

#### 2.1 EFW System

The EFW system consists of two 100-percent capacity trains, the red train and the green train. Each train can supply water to either steam generator and the green train was designed to be totally independent of alternating current (ac) power. Motor-operated valves are installed in the red and green trains, downstream of each pump. These valves have the safety-related function of opening on an EFW actuation signal (EFAS) and closing on a main steam isolation signal. These signals override the normal open/close controls for the valves.

A simplified diagram of the configuration is shown in Attachment 2. Each train has four valves, two for each steam generator. Each of the four lines has two valves, one from each train, in series.

The green train has a turbine-driven pump and uses green train dc power to operate the pump controls. There are four dc motor-operated valves downstream of the pump, with the normally closed green train dc valves nearest the pump and the normally open red train dc valves nearest the steam generators. The red train valves in the green train are normally open and assumed to fail as is (open).

The red train uses a motor-driven pump with red train ac power. There are four motor-operated valves downstream of this pump, with dc power used in the valve control circuit and ac power used to operate these valves. The green train valves in the red train are normally open and were assumed to fail as is (open). Each green train valve uses an energized dc relay in the valve control circuit to keep the valve open and the valve closes when the relay is deenergized.

## 2.2 Vital DC Buses

There are two trains of vital 125-volt dc buses, which provide a reliable source of power to control various breakers and equipment in the plant, including emergency diesel generators (EDG), instrumentation, and ac breakers. Protective tripping and automatic transfer functions for the safety-related 4160 Vac buses is powered from the vital dc buses.

The red train dc bus provides control functions to the red train motor-driven EFW pump, control and protection functions for 4160-Vac Buses 2A1 and 2A3, and control power to EDG A.

The green train dc bus provides control power to the green train turbine-driven EFW pump, control and protective functions to 4160-Vac Buses 2A2 and 2A4, and control power to EDG B. The green train also powers the main turbine electrohydraulic control system and the main generator excitation field breaker.

## 2.3 4160-Vac System

The 4160-Vac system contains electrical Buses 2A1, 2A2, 2A3, and 2A4. Buses 2A1 and 2A2 provide power to nonsafety-related auxiliaries and Buses 2A3 and 2A4 supply power to safety-related equipment. Buses 2A1 and 2A3 are normally connected together and Buses 2A2 and 2A4 are normally connected together.

The main generator supplies power to the main grid by the main transformer and normally to plant loads from the unit auxiliary transformer (UAT). The UAT also normally supplies power to safety-related Buses 2A3 and 2A4. If the main generator trips, a fast transfer of power from the UAT to Startup Transformer 3 is designed to occur to preclude an interruption of power to safety-related components. Startup Transformer 3 remains energized through offsite power sources. If there is a loss of a vital dc bus, the automatic transfer will not occur.

## 3 SINGLE FAILURE SCENARIO

The licensee identified that a single failure of the green train safety-related 125 volt dc bus affects both trains of EFW. This initiating failure also causes a loss of voltage to the main turbine electrohydraulic control system, which causes the main turbine valves to close after a 3-second time delay. After the turbine valves are closed, the main generator output breakers open, but the generator field breaker, which supplies plant loads, does not trip since control power is not available. Therefore, the main generator remains tied to ac Buses 2A2 and 2A4 (green train power) via the UAT. The green train relays, which are energized to open, will close and this will enable the green train valves in the red train EFW to close provided motive ac power is available. AC power would remain available to close these valves due to the designed time delay in the generator trip as well as from the power that continues to be produced during coastdown of the generator.

The designed fast transfer of power to Startup Transformer 3 will not occur due to loss of control power to the affected breakers. Also, the affected EDG will not automatically start due to the loss of the vital dc bus. Shortly thereafter, an EFAS occurs as the steam generator levels decrease due to boiloff. This EFAS is directed to both EFW pumps and an open signal to the eight EFW discharge valves is applied. The green train turbine driven pump is inoperable due to the initiating event, but the red train pump is available and starts. Since the two ac green train valves in the red train EFW had closed, there is no flow path to a steam generator. These valves cannot open from the EFAS, since there is no ac power available. The affected EDG did not start and there is no automatic transfer to the startup transformer due to the initiating event.

This sequence is an unanticipated effect of a postulated loss of the green train vital dc bus on the red train of the EFW. This postulated event occurs because the control power and the motive power for these valves were different, and the failure of the control power did not immediately remove the motive power to these valves. The design intention was that motive power would not be available and, therefore, the green train valves would fail-as-is (open) and a flow path from the red train pump to the steam generator would remain available. The designer of the configuration failed to consider the effect that coastdown of the main generator would have on the ac powered valves.

The licensee also evaluated a postulated loss of the red train vital dc on the EFW system and determined that this failure did not render the green train inoperable. The control power and the motive power are from the same source and, if the source fails, the normally open valves do not move. The inspector verified that, for a loss of the red train dc bus, the green train EFW pump remained operable.

#### 4 SEQUENCE OF EVENTS AND TS CONSIDERATIONS

The following describe the relevant timeline for this event and application of TS action statements.

In December 1983, Design Change Package 82-2160 was implemented. This modification replaced hydraulically-operated valves with motor-operated valves to resolve environmental qualification and valve reliability concerns. This modification inadvertently introduced the single failure concern.

Between March and July 1995, the licensee ran the simulator to verify and validate a revision to Abnormal Operating Procedure (AOP) 2203.037, "Loss of 125 Vdc." In approximately mid-July, the licensee initially identified that the postulated single failure of the loss of green train dc leads to both trains of the EFW being inoperable. After discussion of this situation with the plant staff to determine if the plant were susceptible to this failure, the licensee initiated Condition Report 2-95-0128 on July 19.

The licensee evaluated the situation and concluded that the postulated failure of the green vital dc bus rendered the red train of EFW inoperable. Accordingly, the licensee entered the TS action statement associated with one train of emergency feedwater being inoperable (3.7.1.2), which requires a unit shutdown within 72 hours if the affected train is not restored to operability.

The licensee considered whether the single failure vulnerability placed them in a condition beyond the scope of TS 3.7.1.2, since the single failure affected the operability of both trains. The licensee cited guidance provided in Section 6.3 of Generic Letter 91-18, "Information to Licensees Regarding Two NRC Inspection Manual Sections on Resolution of Degraded and Nonconforming Conditions and on Operability," and concluded that the failure of the red train was consequential to the initiating event and, accordingly, the red train should be declared inoperable. The fact that the initiating event would also render the green train inoperable is not relevant since it is acknowledged that any time one train of a safety system is inoperable, the other train is vulnerable to a single failure. The inspector concluded that the licensee's operability determinations were consistent with the guidance provided in Generic Letter 91-18. The consequential failure of the design basis initiating event of loss of the green train vital dc bus was the inoperability of the red train EFW. Therefore, only the red train of EFW needed to be declared inoperable. The green train EFW was not in a degraded or inoperable status since, by design, it is vulnerable to failure upon the initiating event. Accordingly, TS Action Statement 3.7.1.2 for one train of EFW inoperable was appropriately entered.

Three times in the next 4 days, the licensee switched the safety-related 4160 volt Bus 2A4 and nonsafety-related Bus 2A2 power supplies back to the UAT from Startup Transformer 3 due to lightning in the immediate vicinity of the site. The licensee entered TS 3.7.1.2 each time. The licensee switched the 4160 bus back to Startup Transformer 3 as the thunderstorms left the area and exited the TS action statement.

The licensee switched power supplies from Startup Transformer 3 to the UAT because a lightning strike and loss of Startup Transformer 3 could cause a more complicated plant transient than would occur if the electrical power configuration were through the normal UAT. While using either transformer, the unit would experience a reactor trip. However, if Startup Transformer 3 were supplying Busses 2A2 and 2A4, power would be lost to loads on these buses and the EDG would be challenged to supply the loads. If the UAT were supplying these loads and it was rendered inoperable from a lightning strike, the designed fast transfer to Startup Transformer 3 would occur. This logic, of course, assumes that the loss of the green 125 vdc bus does not occur simultaneously. Since the loss of a dc bus is a very remote event, the licensee considered the transfers which occurred appropriate. Although the licensee's switching of power supply transformers constituted voluntary entry into a TS action statement, which is designed to restrict operation in a mode where redundant safety equipment is inoperable, given the information available at that time, the licensee's actions were not inconsistent with safe operation of the facility and were not precluded by regulatory requirements.

On July 25, the licensee modified the green train valves in the red train EFW control power closing circuitry using Plant Change 95-8057, which removed the single failure concern. This change added a relay into the control circuit, which ensures that, if the green train dc bus fails, the valve will fail-as-is (open). The inspector reviewed the plant change and found it acceptable.

## 5 DESIGN ERROR AND IDENTIFICATION

As previously stated, Design Change Package (DCP) 82-2160 implemented in December 1983 inadvertently introduced the single failure vulnerability. This DCP did not explicitly consider the actual effect of a loss of vital dc on the ac valves, but implicitly assumed that the valves would not move since they would not have motive power. The ac power available from the turbine generator coastdown was not considered. The valves were believed to fail-as-is on loss of dc power. The postmaintenance testing and single failure analysis performed did not identify the design flaw.

The licensee identified this error from a simulator verification and validation of AOP 2203.037, "Loss of 125 Vdc," prior to implementing Revision 2 to this procedure. The licensee was using the simulator to verify whether AOP changes were appropriate.

The first time the licensee verified this AOP was in 1991. At that time the simulator was not capable of modeling the transient. Therefore, the licensee completed the validation of this AOP using "table-top" methods. Upgrades to the simulator computer hardware and software programming since 1991 made it now possible to model this transient.

The inspector reviewed several licensee event reports (LERs) related to design failures since 1984 to see if any of these licensee efforts should have identified this design error. The inspector reviewed the licensee's efforts with the design basis reconstitution program and the licensee's efforts for the electrical distribution safety functional inspection. The inspector concluded that these efforts did not have the scope required to identify this problem.

The inspector also reviewed LERs since 1984 related to the EFW system to determine if any of these LERs should have identified this problem. The inspector did not identify any LERs that should have alerted the licensee of this design flaw. The inspector reviewed condition reports issued since 1990 and did not find any condition reports that appeared related to this issue.

The inspector concluded that there was not a reasonable opportunity to identify this problem.

The licensee committed to the Institute of Electrical and Electronic Engineers Standard 379-1972, "Trial-Use Guide for the Application of the Single-Failure Criterion to Nuclear Power Generating Station Protection Systems." This standard provides guidance on acceptable methods of single-failure analysis. Section 6.4 of this standard, "Actuator Circuit," states, in part, that:

Those actuator circuits designed to fail in a preferred mode upon loss of electric power may be vulnerable to failures that would cause a voltage to be applied to and maintained incorrectly on the actuator system terminals. Such actuator circuits should be analyzed to assure that no single failure could cause a significant loss of function due to an improper connection of the actuator to a source of energy.

This design issue was caused by a failure to fully implement this standard. The inspector examined subsequent enhancements to the licensee's design change procedure and concluded they were adequate to preclude occurrence of a similar design error.

10 CFR Part 50, Appendix B, Criterion III, "Design Control," states, in part, that "measures shall be established to assure that applicable regulatory requirements and the design bases . . . for those structures, systems, and components to which this appendix applies are correctly translated into specifications, drawings, procedures, and instructions." 10 CFR Part 50, Appendix A, Criterion 34, "Residual Heat Removal," requires that systems needed to remove residual heat be designed to meet the single failure criterion. The EFW system is required to remove residual heat from the reactor coolant system, and the implementation of DCP 82-2160 introduced a single failure mechanism that could render both trains of EFW inoperable.

The introduction of the single failure vulnerability into the EFW system is a violation, which the licensee identified and corrected in an expeditious manner. The inspector concluded that this design flaw was subtle, not likely to have been found from other licensee's efforts, and not reflective of current performance in the design change area. Consistent with the guidance contained in Section VII.B.3 of NUREG-1600, "General Statement of Policy and Procedures for NRC Enforcement Actions," enforcement discretion will be exercised and the violation will not be cited.

## 6 IN-OFFICE REVIEW OF LERs

The following LER was closed based on an in-office review. The review verified that the appropriate reporting requirements were met, the licensee took the appropriate corrective actions, and no additional inspection activities were required to review the specific issues:

- LER 368/95-001: Human Error in the Design of a Plant Modification Created the Potential for Failure of One Dc Electrical Bus to Cause the Failure of the Opposite Train of EFW



## ATTACHMENT 1

### 1 PERSONS CONTACTED

#### Licensee Personnel

C. Anderson, Unit 2 Operations Manager  
R. Carter, Assistant Operations Manager  
M. Cooper, Licensing Specialist  
B. Day, Acting Design Engineering Director  
B. Eaton, Unit 2 Plant Manager  
R. Edington, Unit 1 Plant Manager  
D. Felkner, Unit 2 System Engineering  
J. Head, Nuclear Engineering Design Supervisor  
D. Mims, Licensing Director  
T. Mitchell, Unit 2 System Engineering  
L. Schwartz, Electrical & Instrumentation Control Design Engineering Supervisor  
M. Smith, Licensing Supervisor

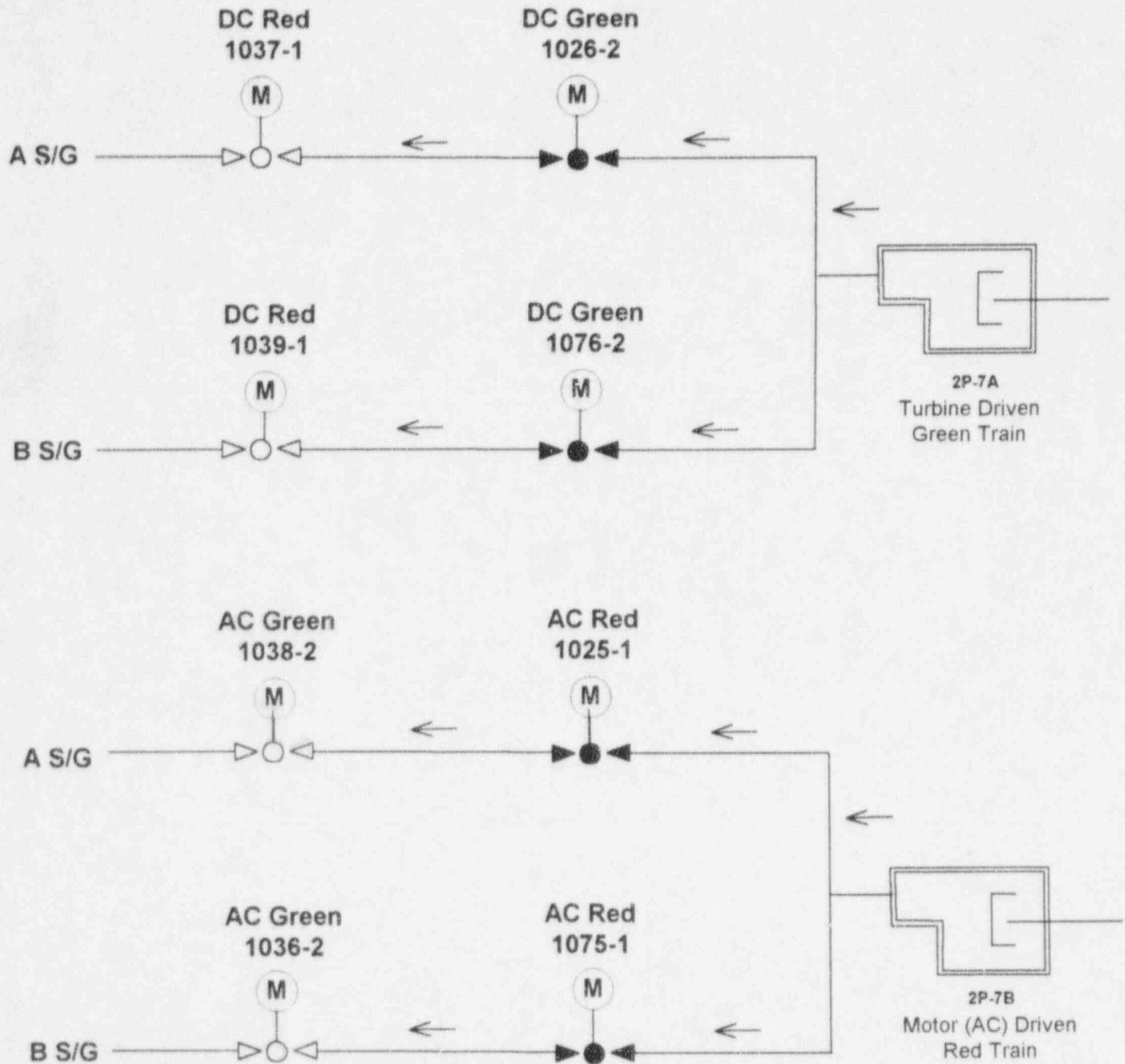
The personnel listed above attended the exit meeting. In addition to these personnel, the inspectors contacted other personnel during this inspection period.

### 2 EXIT MEETING

The inspectors conducted an exit meeting on September 6, 1995. During this meeting, the inspectors reviewed the scope and findings of the report. The licensee did not express a position on the inspection findings documented in this inspection report. The licensee did not identify as proprietary any information provided to, or reviewed by, the inspectors.

# ATTACHMENT 2

## ANO UNIT 2 Emergency Feedwater Simplified Diagram



Shaded valves are normally closed and open on an emergency feedwater actuation signal. Unshaded valves are normally open, but also receive an emergency feedwater actuation signal. Green and red designations indicate the train that the component is associated with. Alternating current valves use dc control circuits.