

DEC 21 1993

Docket No. 50-412

Mr. J. D. Sieber
Senior Vice President
Nuclear Power Division
Duquesne Light Company
Post Office Box 4
Shippingport, Pennsylvania 15077

Dear Mr. Sieber:

SUBJECT: NRC AUGMENTED INSPECTION TEAM (AIT) REGARDING THE
FAILURE OF THE EMERGENCY DIESEL GENERATOR LOAD
SEQUENCERS NRC INSPECTION REPORT 50-412/93-81

The enclosed report refers to the NRC Augmented Inspection Team (AIT), led by Mr. James Trapp of this office, on November 9-19, 1993, at the Unit 2, Beaver Valley Power Station in Shippingport, Pennsylvania. The purpose of this inspection was to review the circumstances regarding the failure of both trains of the emergency diesel generator load sequencers. At the conclusion of the inspection, the team findings were discussed with you and members of your staff at an exit meeting that was open for public observation on December 2, 1993.

The scope of the inspection included developing a detailed event description, evaluating the root causes for the events, assessing the effectiveness of corrective actions, and evaluating the safety significance of the event. The inspection consisted of selective examination of procedures and representative records, observations of testing and inspections, and interviews with personnel.

The failure of both emergency diesel generator load sequencers would prevent automatic initiation of the emergency core cooling systems in the event of an accident with a loss of offsite power. The failure of both load sequencers was a significant event because a common cause resulted in the failure of multiple trains of a system designed to mitigate the consequences of an accident. Based on the safety significance of this event, the NRC dispatched an AIT.

270048

9312280035 XA

1/3/94
record copy

1510
111

DEC 21 1993

Duquesne Light Company

2

The cause for the failure of the load sequencers was determined to be a malfunction of digital microprocessor based timer/relays. The malfunction in the timer/relays was caused by voltage spikes induced when auxiliary relays in the load sequencer circuits were deenergized. Several diodes were installed across relay coils in the load sequencer circuits to reduce the magnitude of the voltage spikes. The AIT reviewed your corrective actions and concluded that the installation of the diodes was an acceptable response to this failure.

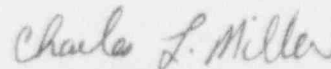
The team concluded that the root cause of the failures was inadequate design control. The modification process that installed the microprocessor based timer/relays in 1990 did not place adequate control on the selection and review for suitability of the new timer/relays. The susceptibility of microprocessor based equipment to voltage disturbances and electromagnetic interference was well known at the time of this design change. It does not appear that adequate detail was provided in the design specification generated for the timer/relays or in the commercial grade qualification testing for these components. Weak design control was also cited as the cause for the failure of six load sequencer timer/relays during the previous failure of the load sequencers in 1992. We are also concerned that during the installation of the diodes, a malfunction was identified during post modification testing with the starting sequence step of the auxiliary feedwater pump. This malfunction required additional design changes to the sequencer and pump starting logic.

Based on the potential of recurring design control issues and the significance of this event, we are planning to schedule an enforcement conference to discuss the circumstances surrounding this issue. The details and schedule for the enforcement conference will be provided in a separate correspondence.

In accordance with 10 CFR 2.790 of the Commission's regulations, a copy of this letter and the enclosed inspection report will be placed in the NRC Public Document Room.

We will gladly discuss any questions you have concerning this inspection.

Sincerely,



Charles L. Miller, Acting Deputy Director
Division of Reactor Safety

Enclosure: NRC Region I Inspection Report No. 50-412/93-81

DEC 21 1993

Duquesne Light Company

3

cc w/encl:

G. S. Thomas, Vice President, Nuclear Services
D. E. Spoerry, Vice President, Nuclear Operations
L. R. Freeland, General Manager, Nuclear Operations Unit
K. D. Grada, Manager, Quality Services Unit
N. R. Tonet, Manager, Nuclear Safety Department
H. R. Caldwell, General Superintendent, Nuclear Operations
K. Abraham, PAO (2)
Public Document Room (PDR)
Local Public Document Room (LPDR)
Nuclear Safety Information Center (NSIC)
NRC Resident Inspector
Commonwealth of Pennsylvania
State of Ohio

DEC 21 1993

Duquesne Light Company

4

bcc w/encl:

Region I Docket Room (with concurrences)

W. Lazarus, DRP

D. Lew, DRP

bcc w/encl (VIA E-MAIL):

W. Butler, NRR

G. Edison, NRR

W. Dean, OEDO

bcc w/encl (AIT REPORTS ONLY):

The Chairman

Commissioner Rogers

Commissioner Remick

Commissioner de Planque

J. Taylor, EDO

T. Murley, NRR

DCD (OWFN P1-37) (Dist. Code #IE10)

A. Chaffee, NRR/DORS/EAB

E. Jordan, AEOD

INPO

P. Boehnert, Chairman, ACRS (AIT Reports Only)

K. Raglin, AEOD (AIT Reports Only)

WI:DRS

Trapp


Trapp
12/13/93



RI:DRS

Durr

12/14/93



RI:DRS

Miller

12/16/93



12/17/93

RI:RA

Martin

12/20/93

OFFICIAL RECORD COPY

A:BV9381.INS

U. S. NUCLEAR REGULATORY COMMISSION
REGION I
AUGMENTED INSPECTION TEAM REPORT

INSPECTION OF EMERGENCY DIESEL GENERATOR
LOAD SEQUENCER FAILURES

REPORT/DOCKET NOS. 50-412/93-81

LICENSE NO. NPF-73

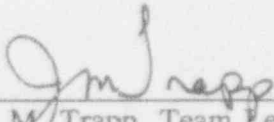
LICENSEE: Duquesne Light Company
One Oxford Center
301 Grant Street
Pittsburgh, PA 15279

FACILITY: Beaver Valley Unit 2

INSPECTION DATES: November 9-19, 1993

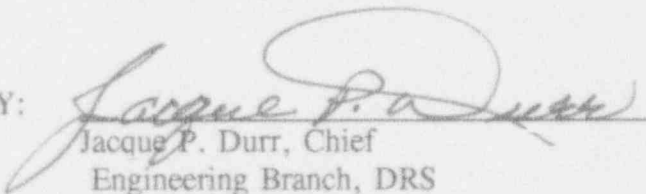
INSPECTORS: J. Calvert, Reactor Engineer, RI
S. Greenlee, Beaver Valley, Resident Inspector
E. Lee, Electrical Engineer, NRR
R. Skokowski, Reactor Engineer, RI

TEAM LEADER:


James M. Trapp, Team Leader
Engineering Branch, DRS

12-13-93
Date

APPROVED BY:


Jacques P. Durr, Chief
Engineering Branch, DRS

12/13/93
Date

~~Q312280038~~

EXECUTIVE SUMMARY

The scope of the Augmented Inspection Team (AIT) inspection was provided by the Region I Regional Administrator in the Augmented Inspection Team Charter. The team was tasked with conducting a detailed review of the circumstances surrounding the failure of both emergency diesel generator load sequencers during routine surveillance testing. Specifically, the team was tasked with developing a detailed sequence of events, evaluating the root cause determination, assessing the effectiveness of the corrective actions, and evaluating the safety significance of the event.

The emergency diesel generator load sequencers automatically place vital safety-related equipment in service if normal power is lost to the emergency busses. Following restoration of power to the emergency busses by the emergency diesel generators, the load sequencer timer/relays are used to load safety-related equipment onto the emergency busses in discrete timed steps. The original load sequencers used electro-mechanical timer/relays to generate the timed steps. The electro-mechanical timer/relays were replaced with digital microprocessor based timer/relays during the second refueling outage, in November 1990. During the third refueling outage, in April 1992, routine surveillance tests identified three of the eight microprocessor timer/relays in each sequencer train had failed. The failures were caused by a modification made to the timer/relays that continuously energized the clock circuits. The root cause for the failures was inadequate design control. The NRC conducted an enforcement conference regarding this failure and issued a Severity Level III violation and a Civil Penalty (NRC Inspection Reports 50-412/92-07 and 50-412/93-22). The failed timer/relays were replaced and the clock circuits were appropriately modified such that the microprocessor timer/relays were only energized during sequencer operation.

On November 4, 1993, during the performance of the Operating Surveillance Test 36.3, "Emergency Diesel Generator Automatic Test," the Train-A, 2-1 emergency diesel generator (EDG) load sequencer failed to automatically load safety-related equipment onto the emergency bus. Subsequent bench testing conducted with the suspect relays was not successful in identifying the cause of the failure. An evaluation of the sequencer logic circuit by the licensee's engineering staff identified two relays, one in the sequencer circuit and one in the solid state protection system, whose malfunction had the potential to cause the symptoms observed during the surveillance test. Both suspect relays were replaced and the surveillance test was successfully repeated on November 5, 1993.

On November 6, 1993, during the performance of the Operating Surveillance Test 36.4, "Emergency Diesel Generator Automatic Test," the Train-B, 2-2 emergency diesel generator load sequencer failed to automatically load safety-related equipment onto the emergency bus. Diagnostic test equipment had been installed on the load sequencer and provided pertinent information on the failure mode. The cause of the sequencer failure was a failed safety injection reset microprocessor timer/relay (762EGSBA). This timer/relay resets the load sequencer when a safety injection signal occurs during a loss of offsite power event. A contact from this timer/relay failed to open, which caused the load sequencer to "lock-up" and fail to automatically load safety-related equipment onto the emergency bus.

The failure of both emergency diesel generator load sequencers would prevent automatic initiation of the emergency core cooling system in the event of an accident with a loss of normal power. In the event that the load sequencers were to malfunction during an accident with a loss of normal power, manual operator actions, in accordance with the emergency operating procedures, would be required to mitigate the consequences of the event. However, for some postulated accidents, manual operator actions might not have been adequate to satisfy the design criteria for the emergency core cooling systems. The team concluded that the common cause failure of multiple trains of a safety system required to mitigate the consequences of an accident was a significant event.

The microprocessor operated timer/relays failed due to voltage spikes introduced through the timer/relay contacts. The voltage spikes were generated by the auxiliary relays that are controlled by the timer/relays. These spikes were generated when the electrical circuit to the coil of an auxiliary relay were opened, resulting in the generation of an "inductive kick," or voltage spike. The "lock-up" of the microprocessors resulted in the failure of the timer/relays. The failure of the timer/relays caused the malfunction of the load sequencers. The exact failure mechanism internal to the microprocessors was not known at the conclusion of this inspection.

A modification of the emergency diesel generator sequencers was implemented to reduce the magnitude of the voltage spikes. The modification installed diodes around the auxiliary relays to reduce the magnitude of the voltage spikes. Nine voltage spike suppression diodes were installed in each emergency diesel generator load sequencer. The post modification testing identified a deficiency with the installation of the diodes. The installation of the diodes increased the drop-out time of the relays, which caused the auxiliary feedwater pump to start at the wrong sequence step. The auxiliary feedwater pump starting circuits and the sequencer logic circuits were modified to correct this problem.

The team concluded that the modification that installed the microprocessor timer/relays was inadequate. The design control for the selection and review for suitability of the Automatic Timer and Controls Company (ATC) timer/relays for this application was not adequate. The modification design inputs should have identified the potential for voltage spiking by the auxiliary relays. This design input should then have been translated into the equipment specification and the dedication testing specification. The delay in auxiliary relay drop-out time caused an auxiliary feedwater pump to start at the wrong sequence step following the installation of the diodes. Further design changes were required to correct this problem. The team concluded that the implications of the installation of the diodes on relay timing was not thoroughly evaluated. The team concluded that the actions taken to correct the auxiliary feedwater pump starting logic problem and the installation of diodes to suppress voltage spikes were acceptable.

TABLE OF CONTENTS

	Page
EXECUTIVE SUMMARY	ii
1.0 INSPECTION SCOPE	1
2.0 DETAILED INSPECTION FINDINGS	2
2.1 Background	2
2.2 Event Description	3
2.3 Safety Significance	4
2.4 Load Sequencer Operation	4
2.5 Root Cause Failure Analysis	5
2.5.1 Sequencer Logic Failure	5
2.5.2 Microprocessor Timer/Relay Failure	6
2.5.3 Engineering Process and Root Cause	7
2.6 Corrective Actions	8
2.6.1 Suppression Diode Installation	8
2.6.2 Auxiliary Feedwater Pump Logic Change	9
2.6.3 Post Modification Testing	11
2.7 Equipment Qualification	12
2.8 Generic Implications	13
2.9 Commitments	15
2.10 Conclusions	15
3.0 EXIT MEETING	16
APPENDIX A - Persons Contacted	
APPENDIX B - Sequencer Operation	
ATTACHMENT 1 - Augmented Inspection Team Charter	
ATTACHMENT 2 - Exit Meeting Slides	
FIGURE 1 - Simplified Sequencer Logic Diagram - Pre-Modification	
FIGURE 2 - Simplified Sequencer Logic Diagram - Post-Modification	

DETAILS

1.0 INSPECTION SCOPE

The scope of the Augmented Inspection Team (AIT) inspection was provided by the Region I Regional Administrator in the Augmented Inspection Team Charter (Attachment 1).

Generally, the team was tasked with conducting a detailed review of the circumstances surrounding the failure, during routine surveillance testing, of both the Train-A and Train-B emergency diesel generator load sequencers. Specifically the team was tasked with:

- Conducting a thorough and systematic review of the circumstances surrounding the failure of the diesel generator load sequencers.
- Collecting, analyzing and documenting factual information to determine the causes, conditions, and circumstances pertaining to the failures, including the adequacy of commercial dedication qualification testing of the relays and the adequacy of the licensee's corrective actions in response to a previous failure of this circuitry.
- Evaluating modification controls, design changes, and surveillance testing which may have contributed to the failures.
- Evaluating the licensee's review of and response to the failures, including implemented and proposed corrective actions.
- Assessing the safety significance of the failures and communicating to Regional and Headquarters NRC management the facts and safety concerns related to problems identified, including single failure vulnerabilities and impact on other safety-related equipment, generic implications and the need for communication of generic issues to other licensees.

In addition to the team charter, the NRC issued a Confirmatory Action Letter (1-93-020) on November 9, 1993, to confirm verbal commitments made by the licensee to the NRC regarding this event. Specifically, the letter documented the following actions: (1) The quarantine and suspension of testing of the relays and components, which may have caused the failure of the emergency diesel generator load sequencers, until resumption is authorized by the AIT team leader; and (2) Maintain Unit 2 in the cold shutdown mode until you receive authorization from the Regional Administrator, NRC Region I.

2.0 DETAILED INSPECTION FINDINGS

2.1 Background

The emergency diesel generator load sequencers automatically place vital safety-related equipment in service in the event that normal power is lost on an emergency bus. If a postulated accident were to occur concurrently with a loss of normal power, then the load sequencers would also automatically place the emergency core cooling system equipment in service. The load sequencer timer/relays are used to distribute the loads being placed on the emergency electrical bus in six discrete timed steps over a 1-minute period. A total of eight timer/relays are installed in each emergency diesel generator load sequencer.

The original emergency diesel generator load sequencer timer/relays were Model ATC 305E electro-mechanical timer/relays manufactured by the Automatic Timer and Controls Company, Incorporated. During the first refueling outage, in 1989, difficulty was encountered with obtaining the necessary set-point repeatability with the electro-mechanical timer/relays. An engineering evaluation was completed to widen the set-point tolerances, thus allowing the Model 305E timer/relays to satisfy the acceptance criteria. Based on the performance of the timer/relays during the first outage, the decision was made to replace these timers during the second refueling outage.

During the second refueling outage, in November 1990, the original timer/relays were replaced with digital Model 365A microprocessor based timer/relays manufactured by the Automatic Timer and Controls Company, Incorporated. The timer/relays were procured as commercial grade components and dedicated by Wyle Laboratories for Class-1E service. To improve the timer/relay performance, the clock circuits were continuously energized on some of the timer/relays in accordance with vendor recommendations. The load sequencers functioned properly during surveillance testing conducted following this modification.

During the third refueling outage, in April 1992, routine surveillance tests identified three of the eight timer/relays in each sequencer train had failed. The failures were caused by the modification made to the timers that continuously energized the clock circuits. Continuously energizing the clock circuits caused overheating and the failure of a resistor in the timer/relays. The clock circuits had been continuously energized to improve the timer/relay set-point accuracy.

The timer/relay configuration was changed based on the vendor's recommendation, but verification of the adequacy of this recommendation was not thoroughly tested or analyzed. The cause of the failures was attributed to inadequate design control. The NRC conducted an enforcement conference regarding this issue and issued a Severity Level III violation and a Civil Penalty (NRC Inspection Reports 50-412/92-07 and 50-412/93-22). The failed timer/relays were replaced and the clock circuits were modified such that the timer/relays were only energized during sequencer operation. The load sequencers tested satisfactorily during the eighteen month surveillance tests conducted at the end of the outage.

2.2 Event Description

On November 4, 1993, during the performance of Operating Surveillance Test 36.3, "Emergency Diesel Generator Automatic Test," the Train-A, 2-1 emergency diesel generator (EDG) load sequencer failed to automatically load the emergency core cooling system equipment on the emergency electrical bus as designed. The routine surveillance test, which is conducted on an eighteen month interval, involved simulating a loss of normal power concurrent with a safety injection signal. During the test, the EDG started and reenergized the associated emergency bus; however, safety-related equipment did not automatically sequence onto the bus as expected. Approximately two minutes following the failure, the safety injection (SI) signal was manually reset. Resetting the safety injection signal caused the safety-related equipment to begin sequencing onto the emergency bus. The surveillance test was terminated and trouble-shooting activities were initiated.

Bench testing of the relays was not successful in identifying the cause of the failure. An evaluation of the sequencer logic circuit by the licensee's engineering staff identified two relays, one in the sequencer circuit and one in the solid state protection system, whose malfunction had the potential to cause the symptoms observed during the failed surveillance test. Both suspect relays were replaced, and diagnostic test equipment was installed to monitor the load sequencer operation. The operating surveillance test was successfully repeated on November 5, 1993. The diagnostic test equipment did not identify any component failures during this test.

On November 6, 1993, during the performance of Operating Surveillance Test 36.4, "Emergency Diesel Generator Automatic Test," the Train-B, 2-2 emergency diesel generator load sequencer failed to automatically load emergency core cooling system equipment on the bus as designed. Diagnostic test equipment had been installed on the load sequencer and provided pertinent information on the failure mode of the sequencer. The cause of the sequencer failure was identified as the safety injection reset relay (762EGSBA). This relay resets the load sequencer if a safety injection signal occurs during a loss of normal power event. A contact from this relay failed to open, which caused the load sequencer to "lock-up" and failed to automatically load equipment onto the emergency bus. Surveillance testing activities were suspended and an evaluation was initiated to determine the cause for the failure.

The operations staff notified the NRC of this failure of multiple trains of a safety system in accordance with 10 CFR 50.72(b)(2)(i) on November 6, 1993. In response, the NRC dispatched an Augmented Inspection Team on November 8, 1993, to review this event.

2.3 Safety Significance

The failure of both emergency diesel generator load sequencers would prevent automatic initiation of the emergency core cooling systems in the event of an accident with a loss of normal power. The automatic initiation of the emergency core cooling systems would have functioned correctly for a postulated accident without the loss of normal power. The load sequencers would also have functioned correctly and loaded safety-related equipment in the event of a loss of normal power without an accident. In the event that the load sequencers were to malfunction during an accident with a loss of normal power, manual operator actions, in accordance with the emergency operating procedures, would be required to mitigate the consequences of the event. The manual actions include locally resetting the motor-control-centers. Resetting the motor-control-centers is required to restore service water to the emergency diesel generators, the high head safety injection pump coolers and to operate essential emergency core cooling system valves. For some postulated accidents, manual operator actions may not have been adequate to satisfy the design criteria for the emergency core cooling systems (10 CFR 50.46). The team concluded that the common cause failure of multiple trains of a safety system required to mitigate the consequences of an accident was a significant event.

At the time of the identification of this failure, Beaver Valley, Unit 2, was in cold shutdown and the automatic initiation of the emergency core system was not required. However, the susceptibility of the timer/relays to this failure mechanism appears to have existed since the microprocessor timer/relays were installed in 1990.

2.4 Load Sequencer Operation

The emergency diesel generator load sequencers automatically load safety-related equipment onto the 4 kV emergency busses following the detection of an undervoltage or degraded voltage conditions on the emergency busses and restoration of power. Additional emergency core cooling system equipment would be placed in service by the load sequencer if the loss of power were to occur concurrently with an accident. The safety-related equipment is loaded onto the diesel generators in six discrete, timed steps, over a 1-minute period, to prevent overloading the diesel generators. The function of the Train-A and Train-B load sequencers is identical. Therefore, only the Train-A sequencer operation will be described.

In the event that power is lost to an emergency bus, the associated emergency diesel generator will automatically start, and the diesel output circuit breaker will close to provide emergency power to the bus. The load sequencer blocks the automatic start function of equipment on the bus so that loads are placed onto the diesel generator in a timed sequence. When the EDG output circuit breaker closes, the load sequencer master relay (3-EGSAAX) energizes (See Figure 1). The master relay starts seven timer/relays that start the timing of sequencer steps 2 through 7. The first step is when the EDG output breaker closes and the seventh step resets the sequencer after 1 minute.

When the timer/relays for steps 2, 3, 5 and 6 time-out, they energize an auxiliary relay, which initiates sequencing of specified loads onto the emergency bus. The step 4 timing relay is slightly different. When it times-out, it energizes a second timer/relay. This slave timer/relay energizes an auxiliary relay for 2 seconds, during which time an auxiliary feedwater pump and/or a quench spray pump may start. The auxiliary feedwater pump and the quench spray pump may also start any time after step 7. Step 7 is the final step in the sequencer, and it resets the load sequencer by deenergizing the master relay (3-EGSAAX).

The load sequencer is designed to reset following a safety injection (SI) or a Phase-B containment isolation (CIB) signal. The reset is required because the loads required during a SI or CIB are different than those required for a loss of normal power alone. Therefore, by resetting the load sequencer, the appropriate equipment is automatically placed in service. If the sequencer receives a reset signal after it has started running, loads already connected to the bus will remain operating. The reset of the load sequencer occurs when the SI reset timer/relay or the CIB reset timer/relay are energized. These relays are energized by engineered safety feature actuation system.

Each train of the load sequencer has eight Automatic Timer Controls, Model 365A microprocessor timer/relays. The microprocessor timer/relays are used for SI and CIB reset, sequence steps 3-6, sequencer reset, and the step 4 slave timer. The step 2 timer is a Model ITE-62K timer/relay manufactured by Asea Brown Boveri (ABB). The Model ITE-62K timer/relay is used for step 2 because of the additional accuracy needed in the timing of this step.

All of the auxiliary relays in the sequencer circuits are Model RXMH-2 electro-mechanical relays. The RXMH-2 relays were manufactured by Asea Brown Boveri.

A detailed description of the load sequencer operation is provided in Appendix B of this inspection report. A simplified logic diagram of the load sequencer circuit is provided in Figure 1.

2.5 Root Cause Failure Analysis

2.5.1 Sequencer Logic Failure

The configuration and operation of the Train-A and Train-B EDG load sequencers are identical; therefore, only the Train-A sequencer operation and failure will be described. The licensee installed diagnostic test equipment on the 2-2 emergency diesel generator load sequencer prior to the performance of the operating surveillance test. Following the failure of the load sequencer, the information collected from the diagnostic test equipment was analyzed to determine the cause.

The cause of the load sequencer failure was determined to be the malfunction of the safety injection microprocessor timer/relay (762-EGSAA) that is used for sequencer reset. Specifically, the microprocessor timer/relay time delay contact opened after a 1/2 second time delay and then inadvertently re-closed a very short time later (approximately 30 milliseconds). Closing of the 762-EGSAA time delay contact energized the 3-EGSAAX4 relay, which "locked-out" (deenergized) the load sequencer master relay and prevented further load sequencer operation.

The diagnostic test equipment also identified that a large negative voltage spike resulted from deenergizing the auxiliary relay (3-EGSAAX4) coil. The auxiliary relay coil (3-EGSAAX4) deenergized when the microprocessor timer/relay (762-EGSAA) time delay contact (762-TDO) opened. The spike was generated by the sudden change in current in the auxiliary relay coil (inductor). The rise and fall times of the voltage spike were very fast and the amplitude of the voltage spike was in excess of 1100 volts at the 762-TDO contact. The voltage spike was transmitted back into the input, power line, and electronics of the microprocessor timer/relay (762-EGSAA) by the arc shower process across the 762-TDO contact. The resulting electronic interference caused the microprocessor to malfunction and reclosed the 762-TDO contact.

2.5.2 Microprocessor Timer/Relay Failure

The licensee conducted a series of bench tests of the microprocessor timer/relays to obtain additional information regarding the failure. The test setup used both a microprocessor timer/relay and an auxiliary relay. These relays were tested in a circuit configuration identical to the in-plant configuration. The results of these bench tests indicated an intermittent failure mode of the microprocessor timer/relays.

The 2-1 load sequencer was temporarily modified to allow the performance of *in situ* testing of the sequencer without starting the safety-related loads. The results of this *in situ* testing indicated an intermittent failure mode of the microprocessor timer/relay (762-EGSAA). These *in situ* tests were instrumented to provide information regarding the magnitude and location of the voltage spikes that occurred during sequencer operation.

The licensee also conducted failure analysis tests internal to the microprocessor timer/relay. The tests concluded that the failure was due to microprocessor malfunction. The cause of microprocessor malfunction was attributed to the negative voltage spikes which were generated when the internal relay deenergized the auxiliary relay coil. The internal relay and contacts (762-TDO) were mounted on the same printed circuit card as the electronic parts and the microprocessor. Consequently, the negative voltage spikes affected the microprocessor and electronic circuitry through an indeterminate transient process involving the internal relay. The exact transient mechanism was not determined at a level below the circuit board indications. The timer/relay vendor engineer stated that symptoms of a microprocessor failure were that the time display malfunctions and the internal timed relay deenergizes, thus causing the normally closed internal timed relay contact to close. Since the

normally closed contact were used in the auxiliary relay circuit, the result was that the auxiliary relay would not be deenergized as required at the end of the microprocessor controlled time delay. This description matched the failure analysis indications. The vendor engineer also stated that the probable cause was due to the inductive discharge of energy across the contacts of the internal relay. This would cause transient arcing and could generate electronic interference internal to the timer/relay, which could cause the microprocessor to malfunction. The inductive energy discharge transient across the contacts is called arc shower and is always a direct consequence of interrupting an inductive current. The licensee plans to send a microprocessor timer/relay to the vendor for additional failure analysis of the electronic circuitry.

Diode suppression of the voltage spikes at the auxiliary relay removed the cause of the arc shower effect and allowed the microprocessor timer/relay to function properly. The effectiveness of diodes in suppressing the voltage spikes created during the deenergization of the auxiliary relays was determined by testing. The microprocessor timer/relay and auxiliary relay were bench tested in the in-plant configuration with the addition of a diode installed in parallel with the coil of the auxiliary relay. The results of these tests showed no failures after approximately 80 operations and indicated a significant reduction in the magnitude of the negative voltage spikes.

The team noted that test results were frequently not well documented. However, the root cause evaluation described and summarized all the testing in a comprehensive, logical manner.

2.5.3 Engineering Process and Root Cause

To determine the root cause of the failure of the emergency diesel generator (EDG) load sequencer the team evaluated the load sequencer circuit design, the failed microprocessor timer/relay (762-EGSAA), and the engineering process for design control.

The licensee's engineering personnel did not suspect that voltage spikes, that normally result from deenergizing auxiliary relays, would present a problem in this application of the microprocessor timer/relay. This was based on their interpretation of the vendor's data sheet, which did not contain any information or precautions that indicated susceptibility of the microprocessor timer/relay to voltage spikes associated with deenergizing auxiliary relays. The licensee did not conduct any confirmatory testing, analysis, or written justification that independently verified the vendor's implied statement concerning the non-susceptibility of the microprocessor timer/relay to voltage disturbances. The team noted that the vendor's data sheet did not discuss noise suppression when using the contacts to control direct current (dc) powered relays. But there were precautions stated for the auxiliary relay. In the auxiliary relay data sheet, the protection of electronic circuits against the auxiliary relay coil inductive voltage type transients was covered along with details of diode suppression techniques.

The modification process and the 10 CFR 50.59 safety evaluation for the modification that installed the microprocessor timer/relays did not list or evaluate inductive spiking as a possible failure mechanism for the microprocessor timer/relays, even though the possibility of spiking existed. Since no suppression techniques were included in the modification, voltage spikes would, therefore, be present and should have been evaluated. The previous failure of the load sequencer in 1992 was attributed to weak design control. At this time, an opportunity was missed to conduct additional design reviews of this modification to determine if other design control deficiencies existed.

The team reviewed the post modification test data from the initial design change and determined that the data did not provide information on load sequencer voltage spikes. The licensee's root cause determination concluded that a more rigorous post modification test may have identified this failure mode.

The team concluded that the effects of the inductive voltage transient which caused arc showering, due to the interruption of an inductive current, were inadequately evaluated in the design process. This resulted in a sequencer design with an inherent failure mechanism that had an extremely high potential for the introduction of a common cause failure.

Therefore, the team attributes the root cause of this event to an inadequate engineering evaluation of the susceptibility of the microprocessor relay/timer to the installed electromagnetic interference (EMI) service conditions. The evaluation did not encompass the EMI sources (such as fast transient voltage spikes/arc shower in this case) or the effect of those EMI sources on the replacement component.

2.6 Corrective Actions

2.6.1 Suppression Diode Installation

Minor design change package (MDCP) number 2057 was developed to prevent the malfunction of microprocessor timer/relays 162-EGSAAX1, 762-EGSAA, 862-EGSAA, 162-EGSBAX1, 762-EGSBA and 862-EGSBA, while the microprocessor timer/relays are deenergizing their respective auxiliary relays. This was accomplished by the installation of inductive voltage transient suppressors across nine auxiliary relay coils in each sequencer train. The sequencer timer/relays and auxiliary relays are located in power panel PNL*SEQ244 for Train-A and in power panel PNL*SEQ254 for Train-B. The applicable portions of the schematics showing the pre-modification and post-modification configurations of the EDG loading sequencer are provided in Figures 1 and 2 of this inspection report, respectively.

The suppressors consisted of diodes which were installed in parallel with the auxiliary relay coils to suppress the voltage spikes created when the relay coils are deenergized. The suppressor type selected was an ABB terminal base mounted, RTXE with the type 2 assembly. These diodes were designed for use with the ABB RXMH-2 type coil relays and other ABB type relays. The purpose of these diodes, as explicitly stated in the published ABB relay data sheets, was "to obtain a dropout delay for dc relays or to protect electronic circuits against transients."

The 10 CFR 50.59 safety evaluation worksheet associated with the modification was reviewed. The safety evaluation identified that the only parameters affected by this change were the voltage and the timing associated with the operation of the sequencer relays. The safety evaluation stated that the addition of a diode to the coil of the ABB RXMH-2 relay delays the dropout time by approximately 20 milliseconds. The safety evaluation concluded that this 20 millisecond delay was not significant compared to the required accuracy of the sequencer, which is on the order of 200 milliseconds. However, the conclusion that the 20 millisecond time delay would not affect sequencer operation was incorrect. A problem with the auxiliary feedwater (AFW) pump start sequence was identified during the performance of the functional test, 2OST-36.3. With the exception of this relay timing problem, the team determined that the MDCP and associated 10 CFR 50.59 evaluation were adequate.

The installation and initial testing of the suppressors for the Train-A load sequencer was completed on November 14, 1993, with the final post-modification testing completed on November 16, 1993. The Train-B diode suppressors were installed and subsequently tested on November 17, 1993. In addition to the installation of the suppressors, microprocessor timer/relays 762-EGSAAX, 862-EGSAAX, and the 862-EGSBAX were replaced.

2.6.2 Auxiliary Feedwater Pump Logic Change

During the performance of the diesel generator 2-1 functional test 2OST-36.3, "Emergency Diesel Generator Automatic Tests," the auxiliary motor driven feedwater (AFW) pump inadvertently started immediately following the closure of the EDG output circuit breaker, rather than at load sequencer step 4. Load sequencer Step 4 equipment is supposed to load 15 to 17 seconds after the emergency diesel output circuit breaker closes. The licensee determined that the cause of the inadvertent start was a delay in the deenergization of auxiliary relay 162-EGSAAX, at the beginning of the loading sequence. The delay in the deenergization of the 162-EGSAAX relay was introduced by the addition of diode suppressors and was not identified during the development of the modification. The AFW pump starting logic is identical for Train-A and Train-B; therefore, only the Train-A starting logic will be described.

AFW Pump Starting Logic Operation

The motor driven auxiliary feedwater pump starting logic consisted of three contacts in series that were all required to close to start the AFW pump. (Not to be confused with the simplified schematic in Figures 1 and 2.) These contacts were closed when voltage was available on the emergency bus, when the load sequencer auxiliary relay 162-EGSAAX was energized (sequencer step 4), and when a safety injection signal was present. The load sequencer relay 162-EGSAAX was normally energized and deenergized when the EDG output circuit breaker closed. This logic was designed to deenergize the 162-EGSAAX relay before the voltage sensing relays on the emergency bus picked-up following power restoration by the EDG. Deenergizing the 162-EGSAAX relay opened a contact in the AFW pump starting logic that prevented starting the AFW pump prior to sequencer step 4. At sequencer step 4, the 162-EGSAAX relay energized and started the AFW pump.

AFW Pump Starting Logic Failure

After the failure of the functional test, the licensee reviewed the AFW pump starting circuit to determine why the AFW pump inadvertently started at sequencer step 1 rather than at step 4. During step 1 of the loading sequence, the safety injection (SI) contact in the AFW pump starting circuit was closed. The two additional contacts in the starting circuit were the 162-EGSAAX contact from the sequencer and the voltage available on the emergency bus contact from the bus voltage sensing relays. To prevent premature starting of the AFW pump, the 162-EGSAAX relay must deenergize prior to the voltage available on the bus sensing relays pick-up. This developed a race between the two relays. The installation of the suppressor diodes around the 162-EGSAAX relay caused a delay in the drop-out time of the 162-EGSAAX relay. This delay allowed the emergency bus voltage relay contacts to close prior to the opening of the 162-EGSAAX contacts, thus starting the AFW pump.

The modification which installed the diode suppressors did not assess the effect of the delay in auxiliary relay drop-out time on the sequencer operation. The ~~original~~ safety evaluation identified that the expected delay in relay drop-out was approximately 20 milliseconds. The safety evaluation correctly stated that this would not adversely affect the overall delay time in loading safety-related equipment. However, the safety evaluation did not document the effect that this would have on the AFW pump start circuit. In addition the functional test measured the actual delay in relay drop-out time to be approximately 70 milliseconds.

Corrective Actions

In response to this failure, the licensee performed a detailed review of the sequencer circuit and verified that no other potential start logic problems existed. In order to correct the failure associated with the AFW pump starting circuit, the licensee initiated an Engineering Change Notice (ECN) to modify the AFW pump starting circuitry such that the 162-EGSAAX relay would not be energized prior to load sequence step 4. The design change

prevents the possibility of having the three AFW pump starting circuit contacts closed prior to sequencer step 4. The 162-EGSAAX relay would be energized for 2 seconds at step 4 of the load sequence. An additional change to the AFW pump start circuit was required to provide a second AFW pump a start signal after the final sequencer step.

Conclusion

The implications of the installation of the diode suppressors on the relay timing were not thoroughly evaluated. Following the installation of the suppressors, the delay in slave relay drop-out time caused the AFW pump to start at the wrong sequence step. An additional design change was required to correct this problem. The team concluded that the actions taken by the licensee to correct this problem were acceptable. However, the team considered the inadequate evaluation of the suppressor installation on relay timing as another example of a weak design control process.

2.6.3 Post Modification Testing

After the installation of the suppressors, the modification design change package required the performance of sequencer testing to verify that the microprocessor timer/relays and the auxiliary relays were functioning properly. The modification design change package required that each sequencer train be tested a total of 30 times. Fifteen cycles were to be initiated by loss of normal power with an SI signal. The remaining fifteen cycles were to be initiated by loss of normal power with a CIB signal. The first and last run for each set of fifteen cycles were to be instrumented to allow for engineering review of the associated traces.

In addition to the testing required for the completion of the modification, other *in situ* tests were performed to verify that the installation of the of the suppression diodes allowed for proper sequencer operation. In total, approximately 200 *in situ* tests were performed with no failures. Whereas, *in situ* testing performed prior to the installation of the suppressors indicated a failure rate of approximately 35%. These post-modification tests verified the operation of the sequencer for loss of offsite power conditions, separately, and with a SI signal or a CIB signal. Approximately 20% of these tests were instrumented to verify that the voltage spikes were adequately suppressed, and to verify that the suppression diodes showed no signs of degradation. The licensee also performed the Operating Surveillance Tests 2OST-36.3 and 2OST-36.4, "Emergency Diesel Generator Automatic Tests," prior to declaring the sequencers operable. The team observed portions of these tests and determined that they were acceptable to demonstrate system operability.

2.7 Equipment Qualification

ATC Timer Relay Dedication

The Beaver Valley Unit 2 Updated Final Safety Analysis Report, Table 8.1-1, lists the Institute of Electrical and Electronic Engineers Standard (IEEE) 323-1974, "Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," as acceptance criteria for Class 1E components. This standard was used as guidance for the dedication of the ATC Model 365A microprocessor timer/relays.

The microprocessor timer/relays were procured as commercial grade items in the spring of 1990 and installed in the load sequencers in the fall of 1990. The dedication of the timer/relays as Class 1E components was controlled through the licensee's engineering design change process rather than through the commercial dedication program. The design change package stated that the following actions were necessary to dedicate the relays:

- A review and evaluation by a third party of the Class 1E environmental qualification of the microprocessor timer/relays. The review and evaluation was to be governed by IEEE 323-1974 (as interpreted by NUREG-0588, Rev. 1) and the seismic qualification requirements of IEEE 344-1975. The environmental qualification parameters specified in the procurement document were: temperature, pressure, humidity, cumulative radiation dose, aging, and seismic forces.
- An initial calibration and checkout of the relays prior to installation.
- A continuity test of the relay circuits to ensure that they were wired properly.
- A functional test of each sequencer circuit.

The third party review and evaluation was complete by Wyle Laboratories. The review was thorough, and provided adequate justification for qualification of the relays as specified in the procurement specification. However, the following deficiencies were noted in the licensee's overall qualification package for the microprocessor timer/relays (the combination of Wyle's testing and the onsite testing) when compared to the requirements of IEEE 323-1974:

- Electromagnetic interference (EMI) was not considered as part of the relay qualification. The term EMI encompasses both external (or radiated) EMI and circuit induced EMI. Section 6.2(2) of IEEE 323-1974 states that Class 1E qualification shall include electromagnetic interference.

- IEEE 323 requires specification of the equipment operating environment. The licensee indicated weakness in this area as illustrated by the following:
 - (1) The equipment performance specifications did not define the transient range of voltage under which the relays were expected to operate.
 - (2) The circuit configuration specified in the procurement specification was not the actual configuration used for all the relays. Some of the installed relays were wired with their clock power supplies continuously energized. The configuration qualified by Wyle had the relays energized only when the sequencer was called on to operate. This eventually led to failure of the relays as discovered in the spring of 1992. This deficiency was covered by Enforcement Action 92-085.
- The qualification documentation was not organized in an auditable form as specified in Section 8 of IEEE 323-1974. The documentation supplied by Wyle was thorough; however, the post-modification test results were not incorporated in the qualification documentation.

Following the sequencer failures on November 4 and 6, 1993, the licensee modified the sequencer design and performed supplemental testing to provide reasonable assurance that the ATC timer/relays installed in the load sequencers would operate as designed. They did not, however, develop an auditable qualification package for the relays. Additionally, no documentation was developed to indicate the status of the ATC timer/relays in the warehouse. The licensee's spare microprocessor timer/relays underwent third party review by Farwell & Hendricks, Inc. Since the spare microprocessor relays do not have auditable qualification documentation, and have not received rigorous testing like the installed relays, their Class 1E qualification requires documentation.

Suppression Diode Dedication

The team reviewed commercial grade evaluation, D-905786, for the suppression diodes. The critical characteristics defined by the licensee were appropriate for the intended application of the suppression diodes. Additionally, the commercial grade evaluation contained appropriate calculations to support the selection of the critical characteristics.

2.8 Generic Implications

Beaver Valley Specific

In addition to the microprocessor timer/relays installed in the sequencers, four additional ATC-365A microprocessor timer/relays are installed in the recirculation spray (RSS) pump starting circuits. These timer/relays start the RSS pumps 628 seconds after the receipt of a containment isolation phase-B (CIB) signal. A failure of the "D" RSS pump occurred during

the performance of surveillance testing during the week of November 1, 1993. The timer/relay started the "D" RSS pump at the time the CIB signal was simulated and did not delay the pump start for 628 seconds. The timer/relay was removed from the circuit for further investigation and bench testing. During bench testing, 125 Vdc was inadvertently applied directly to the timer/relay without a voltage dropping resistor. The voltage dropping resistor was required to reduce the supply voltage to the timer/relay from the 125 Vdc to the design voltage of 24 Vdc. As a result of this error, the timer/relay was destroyed and was not available for further testing. A new timer/relay was installed in the RSS pump starting circuit and a functional test was successfully performed. The team considered the licensee's inadvertent damaging of the failed RSS pump microprocessor timer/relay as an example of weak troubleshooting practices.

Functional test 2BVT1.13.5, "Recirculation Spray Pump Test," was performed, with diagnostic test equipment installed, to determine if voltage spikes were affecting the performance of the RSS pump microprocessor timer/relays. The test identified one negative voltage spike at the microprocessor timer/relay input from the RSS pump breaker trip coil. During accident conditions, the RSS pump would not be tripped until the CIB signal had been reset. When the CIB signal is reset, the RSS pump microprocessor timer/relays are isolated from the RSS pump starting circuit. Therefore, any RSS pump breaker trip coil induced voltage spikes would not adversely affect the microprocessor timer/relay ability to start the RSS pump.

In order to determine if any other solid-state electronic relays had been installed at the Beaver Valley Power Station, the licensee reviewed the category one design change packages (DCPs) implemented over the past five years. This review identified four DCPs that installed solid-state electronic relays. The relays installed by these DCPs were determined to have adequate documentation regarding transient immunity that enveloped the expected transients conditions, or had been appropriately tested for surge withstand capability, fast transient and EMI susceptibility. Therefore, these relays should be suitable for their installed application.

Industry Generic Implications

The team determined that the load sequencer failures at Beaver Valley have generic implications. The generic issue is that licensees must conduct a thorough design review when replacing discrete component electrical devices with digital, microprocessor based electronic devices. Specifically, licensees need to conduct a detailed case-by-case design review to assure that the digital, microprocessor based replacement equipment is compatible for the specific application. This review is necessary since solid state electronic equipment is generally more susceptible to damage from system disturbances than their electromechanical predecessors, particularly with respect to electromagnetic interference and other power supply instabilities.

2.9 Commitments

The first three commitments listed below were provided in the licensee's letter to the NRC, dated November 18, 1993. In addition, the licensee staff stated that a review would be conducted to evaluate the feasibility of additional sequencer testing, and the commercial grade dedication package documentation for microprocessor timer/relays would be upgraded. It is the team's understanding that the licensee plans to do the following:

1. An ATC timer/relay will be sent to the manufacturer for failure analysis.
2. An evaluation of the licensee's capability to identify and specify modification tests which detect functional degradation of modified equipment will be conducted. Until completion of the evaluation, Engineering Assurance and System Engineers will review modification packages prior to installation and will concur with the modification testing requirements.
3. Engineering guidelines will be developed which address engineering requirements for the application of digital solid state components as replacements for non-digital components.
4. A review will be conducted to determine if additional testing of the emergency diesel generator sequencers is feasible and appropriate.
5. The qualification package for the ATC timer/relays will be upgraded to satisfy the IEEE-323-1974 standards. Documentation of the EMI type testing conducted on the ATC relay will be included in the commercial grade qualification package.

2.10 Conclusions

The modification which installed the Model 365A ATC microprocessor timer/relays was inadequate. The design control for the selection and review for suitability of the ATC timer/relays for this application was not adequate. The modification design inputs should have identified the potential for voltage spiking by the auxiliary relays. This design input should then have been translated into the equipment purchase specification and the dedication testing specification.

The implications of the installation of the diodes on relay timing was not thoroughly evaluated. The delay in the slave relay drop-out caused an auxiliary feedwater pump to start at the wrong sequence step following the installation of the diodes. Further design changes were required to correct this problem. The team concluded that the actions taken to correct this problem were acceptable.

The installation of the diodes to suppress voltage spikes was an acceptable corrective action. The team independently verified the test results and concluded that this modification makes the emergency diesel generator load sequencer operable.

Test control and trouble-shooting of the failed relays was weak. For example, the failed relay from the recirculation spray pump was inadvertently destroyed, preventing further investigative testing.

The corrective actions taken in response to the April 1992 clock failures were adequate. However, an opportunity to further evaluate the selection of the microprocessor timer/relays for this service application was missed at this time. The team concluded that the failure mechanism and corrective actions taken in response to the clock failures were independent of the current timer/relay failures.

The qualification documentation for the ATC 365A timer/relays was incomplete. The documentation did not address electromagnetic interference issues and was not put together in an organized and auditable format as specified in IEEE-323-1974.

3.0 EXIT MEETING

The team met with those denoted in Appendix A, on December 2, 1993, to discuss the preliminary inspection findings which are detailed in this report. The exit meeting was open for public observation and the NRC answered public questions following the exit meeting. The slides used at the exit meeting are provided as Attachment 2 of this inspection report.

APPENDIX A

Persons Contacted

Duquesne Light Company

* P. Bienick	Project Engineer
* L. Freeland	General Mgr. Nuclear Operations
* K. Grada	Mgr. Quality Services Unit
* K. Halliday	Director, Electrical Engineering
* F. Lipchick	Sr. Licensing Supr.
* D. McBride	System Engineer
* D. McLain	Mgr. Maintenance Engineering and Assessment
* T. Noonan	Gen. Mgr., Nuclear Engineering and Safety
* D. O'Neil	Gen. Mgr. Public Affairs
* J. Sasala	Director, Nuclear Communication
* R. Scheib	ANSS Unit 2
* J. Sieber	Sr. Vice President - Nuclear Power Division
* M. Siegel	Mgr. Nuclear Engineering Department
* G. Storolis	NSS Unit 2
* D. Szucs	Sr. Engineer, Nuclear Safety
* G. Thomas	Division Vice President - Nuclear Service
* N. Tonet	Mgr. Nuclear Safety
* G. Zupic	Supr. Reactor Engineering

U. S. Nuclear Regulatory Commission

* G. Edison	Project Manager, NRR
* C. Miller	Deputy Division Director, DRS
* L. Rossbach	Sr. Resident Inspector - Beaver Valley

Other

* G. Morris	Video Photographer
* J. Musala	Reporter
* B. Shaw	DLC-retired
* R. Barkanic	Nuclear Engineer, Pa. State DER/BRP

Asterisk (*) denotes those present at the exit meeting conducted on December 2, 1993. The persons contacted list is not a comprehensive list of every individual contacted but provides the principal staff associated with this event.

APPENDIX B

SEQUENCER OPERATION

The following provides a description of the function of the emergency diesel generator load sequencer operation. The Train-A and Train-B load sequencer operations are identical; therefore, only the Train-A sequencer operation will be described. A simplified logic diagram of this circuit is provided in Figure 1 of this inspection report.

Sequencer Operation

1. A loss of offsite power will result in the opening of the normal supply circuit breakers to the emergency bus and the automatic start of the associated emergency diesel generator. The opening of the normal supply circuit breaker to the emergency bus will cause the 52S-ENSAC contact to close.
2. Following the EDG attaining rated speed and voltage, the EDG output circuit breaker closes and contact 52S-ECPAA closes. This energizes master relay, 3-EGSAAX, because the 69-EGSAA and the 3-EGSAAX4 contacts are normally closed. Once the master relay is energized, its associated contacts in the circuits for the slave timer/relays are closed allowing the loads to sequence on in the proper order.
3. When an SI signal is present, contact SIS-K610XA would close.
4. The closing of contact SIS-K610XA provides power to the microprocessor timer/relay 762-EGSAA.
5. When microprocessor timer/relay 762-EGSAA energizes, its timer operation is started, and its normally open 762-INST contact closes.
6. At the closing of contact 762-INST, the SI/CIB reset relay, 3-EGSAAX4, energizes.
7. When relay 3-EGSAAX4 energizes, its normally closed contact in the master relay circuit opens, deenergizing the master relay and consequently all of its slave timer-relays.
8. At 0.5 seconds after energization of the 762-EGSAA microprocessor timer/relay (step 3 above), its normally closed 762-TDO contact opens, deenergizing the SI/CIB reset relay, 3-EGSAAX4. The 762-TDO contact stays open until the 762-EGSAA microprocessor timer/relay is reset (i.e. deenergized).
9. When the 3-EGSAAX4 relay deenergizes, its normally closed contact, which was opened as described in step 5 above, recloses and reenergizes the master relay, 3-EGSAAX, and all its slave timer/relays. Energizing these slave timer/relays allows the safety equipment to load in the proper sequence.

ATTACHMENT 1

AUGMENTED INSPECTION TEAM CHARTER



UNITED STATES
NUCLEAR REGULATORY COMMISSION
REGION I
475 ALLENDALE ROAD
KING OF PRUSSIA, PENNSYLVANIA 19406-1415

File

Docket No. 50-412

NOV 9 1993

MEMORANDUM FOR: Marvin W. Hodges, Director, Division of Reactor Safety


FROM: Thomas T. Martin, Regional Administrator

SUBJECT: AUGMENTED INSPECTION TEAM CHARTER FOR REVIEW OF COMMON MODE FAILURE OF THE EMERGENCY DIESEL GENERATOR LOAD SEQUENCERS AT BEAVER VALLEY UNIT 2

On November 4, 1993, during the load sequencing test of the 2-1 emergency diesel generator (EDG), the load sequencer malfunctioned in such a manner as to prevent automatic loading of the EDG. On November 6, 1993, a load sequencer malfunctioned on the 2-2 EDG. Subsequent testing revealed that a common-mode problem exists that may have prevented either EDG from loading automatically. In order to assess the safety significance of the issue, I have determined that an Augmented Inspection Team (AIT) should be initiated to review the causes and safety implications associated with these malfunctions.

The Division of Reactor Safety (DRS) is assigned the responsibility for the overall conduct of this Augmented Inspection. Jim Trapp, Team Leader, DRS, is appointed as Augmented Inspection Team Leader. Other AIT members are identified in Enclosure 2. The Division of Reactor Projects (DRP) is assigned the responsibility for resident and clerical support, as necessary; and the coordination with other NRC offices, as appropriate. Further, the Division of Reactor Safety, in coordination with DRP is responsible for the timely issuance of the inspection report, the identification and processing of potentially generic issues, and the identification and completion of any enforcement action warranted as a result of the team's review.

Enclosure 1 represents the charter for the Augmented Inspection Team and details the scope of the inspection. The inspection shall be conducted in accordance with NRC Management Directive (MD) 8.3, NRC Inspection Manual 0325, Inspection Procedure 93800, Regional Office Instruction 1010.1, and this memorandum.


Thomas T. Martin
Regional Administrator

Enclosures:

1. Augmented Inspection Team Charter
2. Team Membership

Marvin W. Hodges

2

NOV 9 1993

cc w/encls:

J. Taylor, EDO
J. Sniezek, OEDO
T. Murley, NRR
J. Calvo, NRR
C. Rossi, NRR
W. Butler, NRR
F. Miraglia, NRR
C. McCracken, NRR
J. Wermiel, NRR
W. Russell, NRR
J. Wiggins, NRR
A. Thadani, NRR
B. Grimes, NRR
S. Varga, NRR
B. Boger, NRR
E. Jordan, AEOD
D. Ross, AEOD
V. McCree, OEDO
W. Kane, DRA, RI
R. Cooper, DRP, RI
W. Lanning, DRP, RI
C. Miller, DRS, RI
W. Lazarus, DRP, RI
W. Hehl, DRSS, RI
S. Shankman, DRSS, RI
L. Rossbach, SRI, Beaver Valley
G. Edison, NRR
C. Sisco, DRS, RI
L. Bettenhausen, DRS, RI
J. Linville, DRP, RI
K. Abraham, PAO, RI
M. Miller, SLO, RI

ENCLOSURE 1

AUGMENTED INSPECTION TEAM (AIT) CHARTER

The general objectives of this AIT are to:

1. Conduct a thorough and systematic review of the circumstances surrounding the failure of the diesel generator load sequencers.
2. Collect, analyze, and document relevant factual information to determine the causes, conditions, and circumstances pertaining to the failures, including the adequacy of commercial dedication qualification testing of the relays and the adequacy of the licensee's corrective actions in response to a previous failure of this circuitry (IR 50-412/92-07).
3. Evaluate the licensee's review of and response to the failures, including implemented and proposed corrective actions.
4. Assess the safety significance of the failures and communicate to Regional and Headquarters management the facts and safety concerns related to problems identified, including single failure vulnerabilities, impact on other safety systems, generic implications and the need for communication of generic issues to other licensees.
5. Evaluate modification controls, design changes, and surveillance testing which may have contributed to the failures.
6. Prepare a report documenting the results of this review for the Regional Administrator within thirty days of the completion of the inspection.

ENCLOSURE 2

AIT MEMBERSHIP

James Trapp, AIT Leader, Division of Reactor Safety (DRS), Region I (RI)

John Calvert, Reactor Engineer, Division of Reactor Safety (DRS), RI

Scott Greenlee, Resident Inspector, Beaver Valley Unit 1, DRP, RI

Richard Skokowski, Reactor Engineer, DRS, RI

Eric Lees, NRR

Other NRC personnel, consultants, or contractors will be engaged in this AIT, as needed.

ATTACHMENT 2
AUGMENTED INSPECTION TEAM
EXIT MEETING SLIDES



**AUGMENTED INSPECTION TEAM
BEAVER VALLEY UNIT 2**

**EMERGENCY DIESEL GENERATOR LOAD
SEQUENCER FAILURES**

NRC INSPECTION 50-412/93-81

EXIT MEETING

**DECEMBER 2, 1993
10 a.m.**

- **EXIT MEETING BETWEEN NRC AND LICENSEE.**
- **NRC WILL ADDRESS PUBLIC QUESTIONS REGARDING TEAM FINDINGS.**

BEAVER VALLEY UNIT 2
LOAD SEQUENCER FAILURES

INSPECTION SCOPE

- CONDUCT A THOROUGH AND SYSTEMATIC REVIEW OF THE CIRCUMSTANCES SURROUNDING THE FAILURE.
- COLLECT AND ANALYZE FACTUAL INFORMATION, INCLUDING THE COMMERCIAL GRADE DEDICATION OF THE FAILED TIMER/RELAYS.
- REVIEW THE ADEQUACY OF THE CORRECTIVE ACTIONS TAKEN IN RESPONSE TO THE PREVIOUS SEQUENCER FAILURE.
- REVIEW THE PROPOSED CORRECTIVE ACTIONS.
- EVALUATE THE MODIFICATION AND ANY SURVEILLANCE TESTING THAT MAY HAVE CONTRIBUTED TO THIS FAILURE.
- ASSESS THE SAFETY SIGNIFICANCE OF THE FAILURES.
- DETERMINE IF THIS EVENT HAS GENERIC IMPLICATIONS.

BACKGROUND

- EMERGENCY DIESEL GENERATOR LOAD SEQUENCER AUTOMATICALLY STARTS EQUIPMENT REQUIRED TO MITIGATE THE CONSEQUENCES OF AN ACCIDENT WHEN OFFSITE POWER IS LOST.
- ORIGINALLY THE TIMER/RELAYS WERE ATC MODEL 305E AND WERE NOT MICROPROCESSOR BASED.
- DURING REFUELING OUTAGE (RFO) 2, IN 1990, THE TIMER/RELAYS WERE REPLACED WITH MICROPROCESSOR BASED ATC MODEL 365A TIMER/RELAYS.
- IN 1992 SIX ATC TIMERS WERE IDENTIFIED AS FAILED DUE TO INTERNAL CIRCUIT CLOCK FAILURES.
- THE NRC ISSUED A SEVERITY LEVEL III VIOLATION AND CIVIL PENALTY IN RESPONSE TO THE ATC TIMER/RELAY CLOCK FAILURES.

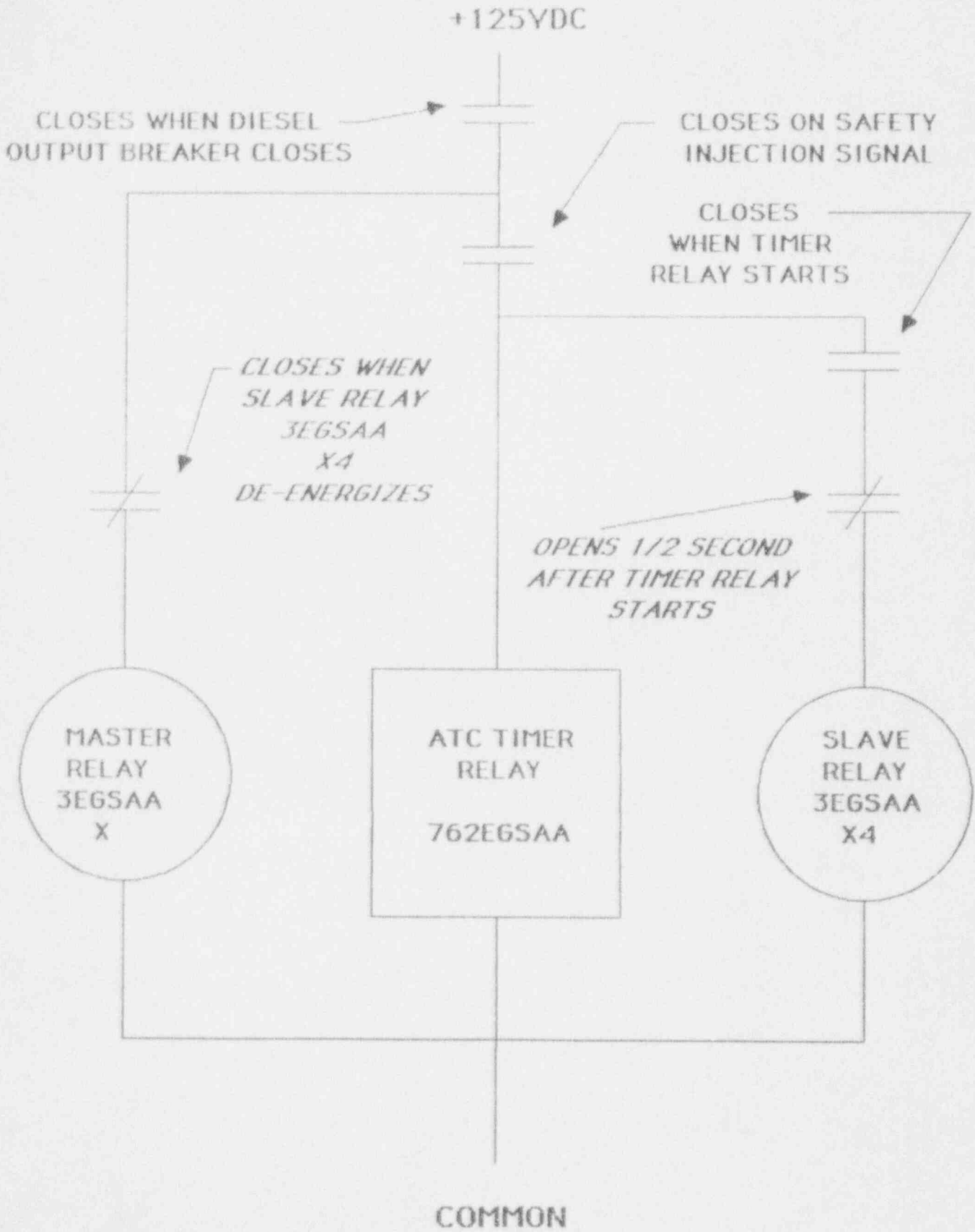
EVENT DESCRIPTION

- ON NOVEMBER 4, 1993, DURING ROUTINE SURVEILLANCE TESTING, THE 2-1 EMERGENCY DIESEL GENERATOR LOAD SEQUENCER FAILED TO FUNCTION.
- ATC TIMER/RELAY 762 WAS REPLACED AND THE SURVEILLANCE TEST WAS SUCCESSFULLY COMPLETED.
- ON NOVEMBER 6, 1993, DURING ROUTINE SURVEILLANCE TESTING, THE 2-2 EMERGENCY DIESEL GENERATOR LOAD SEQUENCER FAILED TO FUNCTION.
- THE LICENSEE NOTIFIED THE NRC OF THE FAILURES ON NOVEMBER 6, 1993.
- IT APPEARED THAT A COMMON CAUSE FAILURE HAD AFFECTED MULTIPLE TRAINS OF A SAFETY SYSTEM.
- AN AIT WAS DISPATCHED BY THE NRC REGIONAL ADMINISTRATOR AND ARRIVED ONSITE ON NOVEMBER 9, 1993.

SAFETY SIGNIFICANCE

- THE DIESEL GENERATOR LOAD SEQUENCER WOULD NOT AUTOMATICALLY START EMERGENCY EQUIPMENT.
- THE FAILURE WOULD ONLY OCCUR DURING A LOSS OF OFFSITE POWER WHEN A SAFETY INJECTION WAS REQUIRED.
- MANUAL OPERATOR ACTIONS WOULD BE REQUIRED TO LOAD SAFETY-RELATED EQUIPMENT.
- RESETTING OF THE MOTOR-CONTROL-CENTERS WOULD REQUIRE OPERATOR ACTIONS FROM OUTSIDE THE CONTROL ROOM.
- THE TEAM DETERMINED THAT THE SAFETY SIGNIFICANCE OF THIS EVENT WAS HIGH BECAUSE A COMMON CAUSE FAILED REDUNDANT TRAINS OF SAFETY-RELATED EQUIPMENT.

DIESEL GENERATOR SEQUENCER LOGIC



CORRECTIVE ACTIONS

- A NUMBER OF BENCH AND INSITU TESTS WERE PERFORMED TO DETERMINE THE CAUSES OF THE EQUIPMENT FAILURE.
- DIODES WERE INSTALLED AROUND THE SLAVE RELAYS TO REDUCED THE MAGNITUDE OF THE VOLTAGE SPIKES CAUSED BY THE DROPOUT OF THESE RELAYS.
- THREE ATC TIMER\RELAYS IN THE SEQUENCER WERE REPLACED WITH NEW TIMER/RELAYS.
- POST MODIFICATION TESTING IDENTIFIED A PROBLEM WITH THE AUXILIARY FEEDWATER PUMP STARTING LOGIC.
- ADDITIONAL SEQUENCER AND PUMP STARTING LOGIC DESIGN CHANGES WERE REQUIRED TO ELIMINATE THE AUXILIARY FEEDWATER PUMP LOGIC PROBLEM.
- EXTENSIVE POST MODIFICATION TESTING OF THE LOAD SEQUENCERS WAS CONDUCTED TO DEMONSTRATE OPERABILITY AND RELIABILITY.

GENERIC IMPLICATIONS

- THE LICENSEE REVIEWED DESIGN CHANGES MADE TO BOTH BEAVER VALLEY 1 AND 2 TO VERIFY NO SIMILAR CONDITIONS EXISTED.
- A DESIGN CHANGE MADE TO THE RECIRCULATION SPRAY PUMP LOGIC WAS IDENTIFIED AS CONTAINING SIMILAR ATC TIMER/RELAYS.
- THE SPIKES IDENTIFIED IN THE RECIRCULATION SPRAY PUMP LOGIC WERE DETERMINED TO NOT AFFECT ATC TIMER/RELAY OPERATION.
- THE NRC IS CURRENTLY PLANNING TO ISSUE AN INFORMATION NOTICE DESCRIBING THIS EVENT.

COMMITMENTS

- A FAILURE ANALYSIS WILL BE CONDUCTED ON AN ATC TIMER/RELAY.
- THE FEASIBILITY OF ADDITIONAL SEQUENCER TESTING WILL BE INVESTIGATED.
- THE QUALIFICATION PACKAGE FOR THE ATC TIMER/RELAYS WILL BE UPGRADED.
- AN EVALUATION OF POST MODIFICATION TESTING WILL BE CONDUCTED.
- ENGINEERING GUIDELINES FOR REPLACEMENTS WITH DIGITAL SOLID STATE COMPONENTS WILL BE DEVELOPED.

CONCLUSIONS

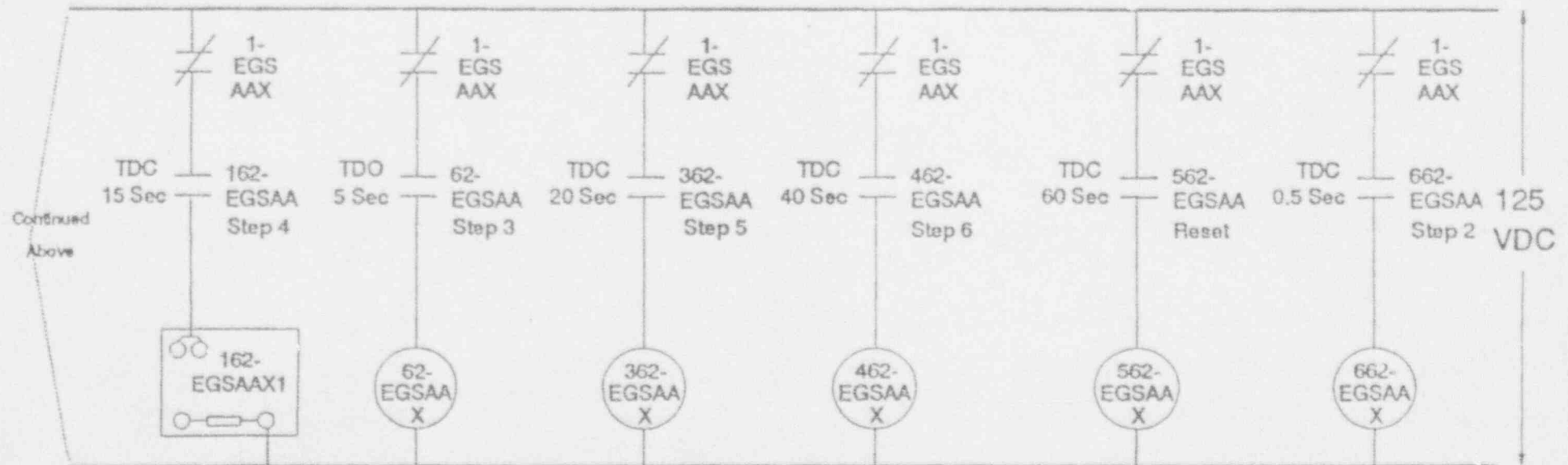
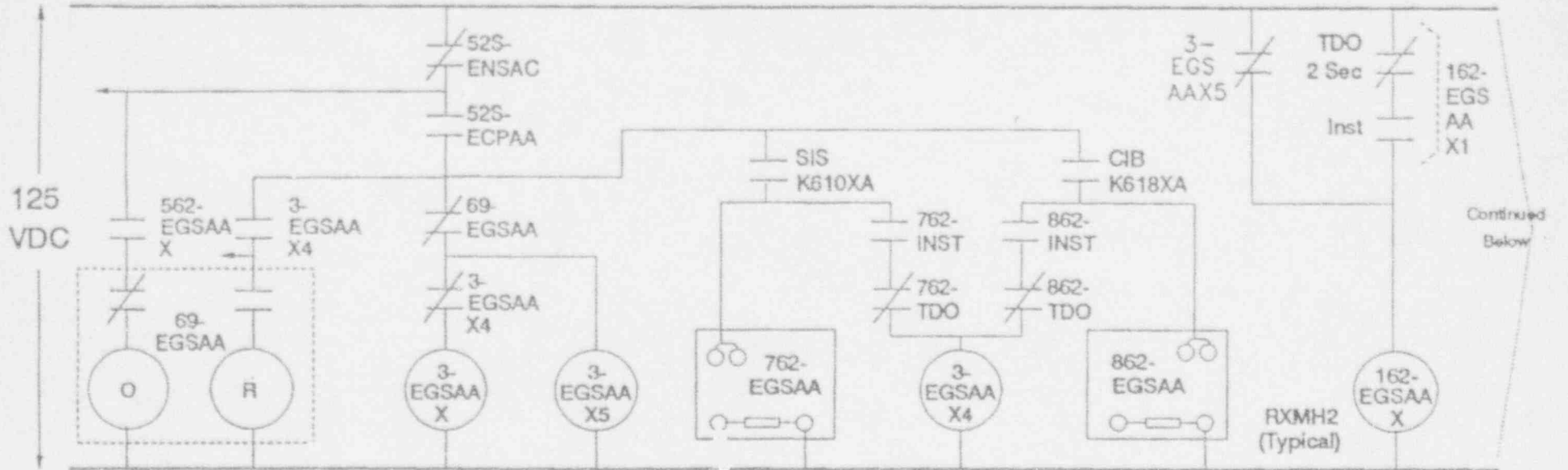
- THE MODIFICATION THAT INSTALLED THE MODEL 365A, ATC TIMER/RELAYS WAS INADEQUATE.
- A WEAK TECHNICAL UNDERSTANDING OF THE MODEL 365A TIMER/RELAY LIMITATIONS, APPLICATIONS AND SPECIFICATIONS IN THE ENGINEERING DEPARTMENT WAS THE ROOT CAUSE FOR THIS FAILURE.
- THE CORRECTIVE ACTION THAT INSTALLED DIODES TO SUPPRESS THE VOLTAGE SPIKES WAS ACCEPTABLE.
- TROUBLE-SHOOTING ACTIVITIES AND TESTING FOLLOWING THE FAILURE WERE POORLY PLANNED AND WERE FREQUENTLY NOT FORMALLY DOCUMENTED.
- THE QUALIFICATION DOCUMENTATION FOR THE ATC TIMER/RELAYS WAS INCOMPLETE.
- THE CORRECTIVE ACTIONS TAKEN IN RESPONSE TO THE PREVIOUS CLOCK CIRCUIT FAILURE WERE APPROPRIATE AND WERE INDEPENDENT OF THE CURRENT FAILURE.

ENFORCEMENT ACTIONS

- AN NRC ENFORCEMENT CONFERENCE WILL BE SCHEDULED TO DISCUSS THE EVENTS AND CIRCUMSTANCES SURROUNDING THE FAILURE OF THE EMERGENCY DIESEL GENERATOR LOAD SEQUENCERS.

Figure 1

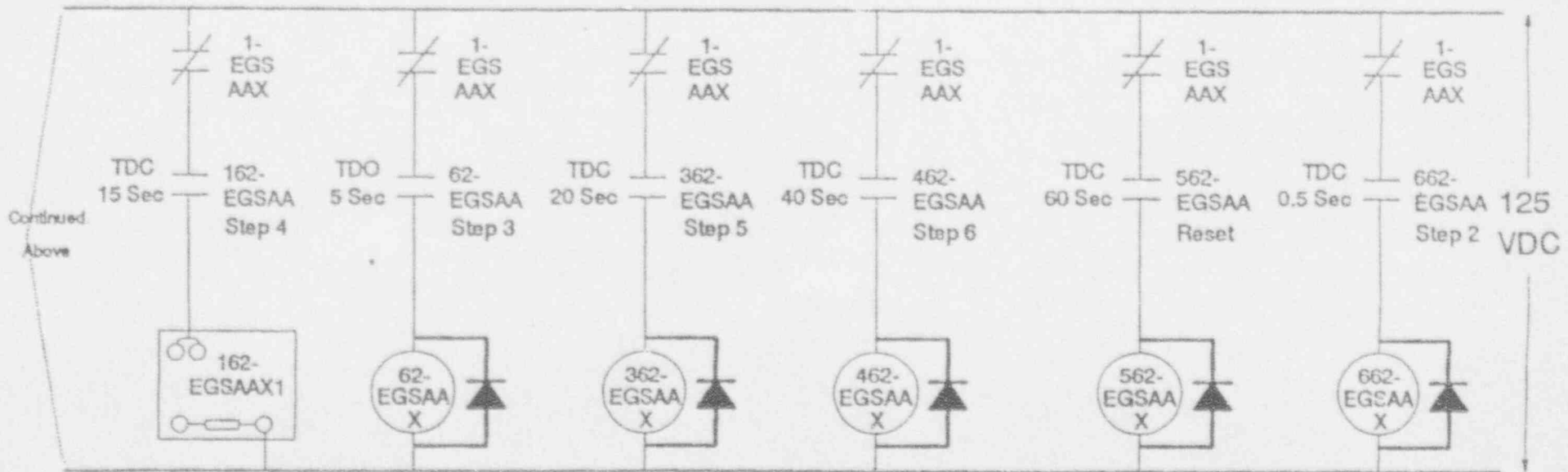
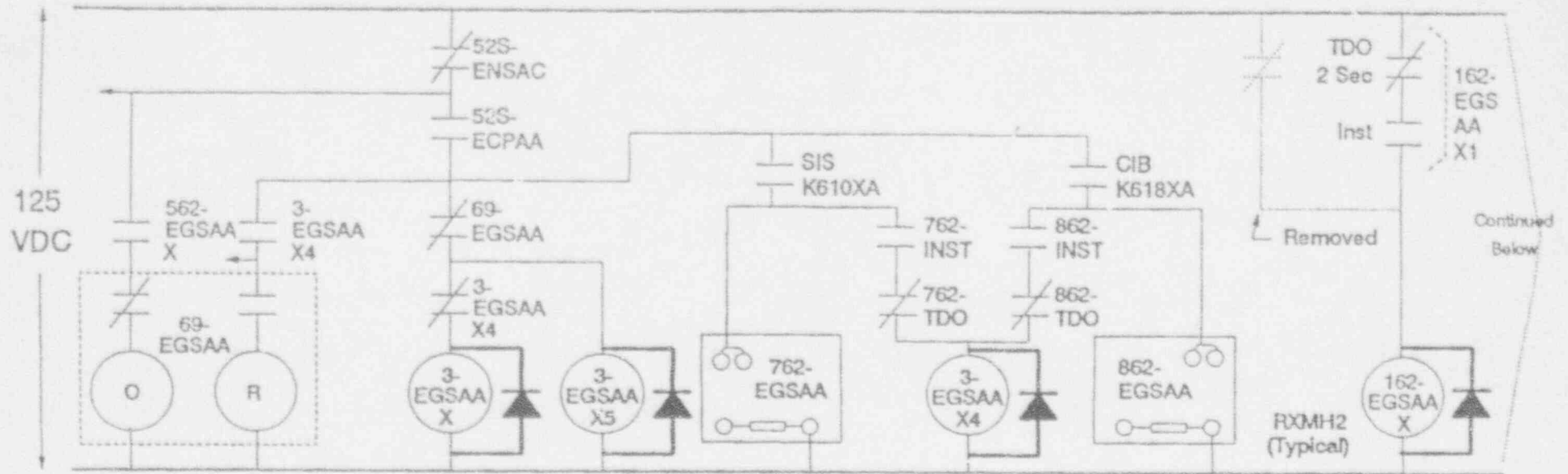
12241-E-12A Sh.1 (Simplified) - Before Modification



Timers for 62, 162, 362, 462, 562, 662 not shown

Figure 2

12241-E-12A Sh.1 (Simplified) - After Modification



Timers for 62, 162, 362, 462, 562, 662 not shown