A-167

GPC-167

DOCKETED
USNRC

'95 SEP -8 P4:04

OFFICE OF SECRETARY
DOCKETING & SERVICE
BRANCH

APPENDIX J

DIESEL GENERATOR FAILURE REVIEW AND ANALYSIS

NUCLEAR REGULATORY COMMISSION GPC
Docket No. 50-424/425-OLA-3 EXHIBIT NO. II-167
In the matter of Ga Power / Vogtle
☐ Staff ☑ Applicant ☐ Intervenor ☐ Other
☐ Identified ☑ Received ☐ Rejected Reporter WLW
Date 8-24-95 Witness Odyoung / Johnston

CONTENTS

APPENDIX J

DIESEL GENERATOR FAILURE REVIEW AND ANALYSIS

APPENDIX J

DIESEL GENERATOR FAILURE REVIEW AND ANALYSIS

This appendix describes the scope and results of the licensee's investigation to determine the causes for the unexpected 1A emergency diesel generator shutdowns during the incident. It describes the maintenance performed on the emergency diesel generator during the refueling outage before the event, the post-incident review and troubleshooting efforts, and the sensor testing program to determine the root cause of the sensor malfunctions.

1 ACTIVITIES INVOLVING THE EMERGENCY DIESEL GENERATOR BEFORE THE INCIDENT

Vogtle Unit 1 was shut down during the last week of February 1990 to enter its second refueling outage. Activities scheduled during the outage included surveillance testing of the two Unit 1 emergency diesel generators. Section 4.8.1.1.2h of the Vogtle Unit 1 Technical Specifications lists the surveillance testing that is required for the emergency diesel generators once every 18 months during plant shutdown. The licensee performs this surveillance during each refueling outage. The required 18-month surveillance tests performed included (1) inspections in accordance with the manufacturer's recommendations, (2) tests to determine if the emergency diesel generators respond adequately to load rejections, simulated losses of offsite power (LOOP), and simulated engineered safety features actuation signals (i.e., safety injection signals), both with and without LOOP, (3) a 24-hour test run, and (4) other operability, system alignment and sequencer tests.

Much of the surveillance during the outage was performed in accordance with GPC Procedure No. 28713-1, "Second End of Cycle Diesel Generator Checkout." The procedure includes provisions for measuring and recording engine operating data (e.g., temperatures and pressures) to be used for assessing engine performance and for trend analysis. It also includes instructions for disassembly and inspection of engine equipment and internals (e.g., fuel injectors, air start valves, fuel pumps, governor drive assembly). The procedure specifies (1) inspections and preventive maintenance of the emergency diesel generator starting air and control air systems, (2) calibration of the engine-mounted sensors that can initiate automatic shutdown of the emergency diesel generator to protect the engine under abnormal operating conditions, (3) functional testing of the emergency diesel generator pneumatic and electric control and logic circuits located in the local engine control panels, and (4) engine operation and post-run inspections to be completed before the emergency diesel generators are returned to service. GPC Procedure 27563-C, "Generator and Engine Control Panel Functional Test," is used to test the logic circuits.

Before the second refueling outage, emergency diesel generator 1A was being tested monthly for operability as required by the Vogtle Unit 1 Technical Specifications. Testing is required monthly unless the emergency diesel generator has experienced 2 or more failures in the previous 20 starts or 5 or more failures in the previous 100 starts, in which case operability testing must be performed on a weekly basis. The emergency diesel generator operability testing is performed in accordance with GPC Procedure No. 14980-1, "Diesel Generator Operability Test." The test verifies that acceptable voltage and frequency are attained within a specified time (11.4 seconds) after start of the emergency diesel generator, that the emergency diesel generator will operate in a loaded condition (6800 to 7000 kW) for 60 minutes, and that the diesel generator can be aligned to provide power to its associated safety bus. The licensee has indicated that emergency diesel generator 1A performed successfully during the monthly operability tests preceding the outage.

Between February 27, 1990, and March 1, 1990, emergency diesel generator 1A was started approximately 8 times. Most of the starts were made to support the 18-month testing required by the plant Technical Specifications. The last several starts were made to allow recording of engine data (e.g., maximum firing pressures) and included an 8-hour run. Emergency diesel generator 1A was tagged out of service and declared inoperable later on March 1, 1990. From March 1 to March 12, 1990, the licensee performed tests, inspections, calibrations, and modifications to emergency diesel generator 1A and its support systems. The work performed is specified and tracked, and the results are documented in maintenance work orders. Specific work performed included the following:

- Calibration of the engine-mounted pneumatic sensors used for automatic shutdown of the emergency diesel generator: most of these sensors are manufactured by California Controls Company (Calcon),

- Calibration of the pneumatic pressure switches located in the local engine control panel that provide the interface between the pneumatic and electric portions of the engine control system (e.g., for alarms, permissives); these switches are manufactured by Barksdale Corporation,

- Replacement of the o-rings, gaskets, and 5-micron air filter in the control air regulator and filter assembly, and verification of adequate control air pressure,

- Functional testing of the pneumatic logic elements in the local engine control panel to verify their capability to perform the required start, run, and stop sequences necessary for proper emergency diesel generator operation, and

- Servicing the emergency diesel generator starting air compressors and dryers, including air filter checks and dew point measurements.

During the outage, much of the work on the emergency diesel generators was performed in accordance with commitments made by Georgia Power Company's (GPC's) Nuclear Safety and Compliance Group. These commitments were largely based on recommendations documented in the Design Review and Quality Revalidation Report prepared for GPC by the TDI Diesel Generator Owners' Group. The work performed is designed to ensure the structural and mechanical integrity of engine equipment and to ensure adequate preventive maintenance to provide continued operability.

Emergency diesel generator 1A was returned to service on March 12, 1990, but was not declared operable until operability testing was successfully completed on March 13, 1990. The diesel generator was started at least six times between March 12 and March 13, 1990. Most of the starts were for functional testing in accordance with a temporary one-time test procedure (T-ENG-90-09). The procedure was written to verify proper operation of the governor, proper setting of the overspeed trip devices, and proper operation of the emergency diesel generator in the isochronous mode (i.e., with the emergency diesel generator providing the sole source of power to its bus). The emergency diesel generator is paralleled with offsite power during operability testing. Some of the starts were to repeat tests performed at the beginning of the outage (e.g., manual loading and unloading and load rejection tests) because the plant engineering staff believed it was necessary to redemonstrate proper operation following the disassembly, inspection, and reassembly of engine components. Emergency diesel generator 1A was declared operable on March 13, 1990, after successfully completing the monthly operability test. It was out of service for twelve days.

The licensee is not aware of any unusual alarm conditions or problems that occurred during the testing. The tests included an engine run in excess of 8 hours, and another run in excess of 4 hours. All attempted starts were successful. No engine shutdowns were initiated from the engine-mounted pneumatic trip sensors. After emergency diesel generator 1A was declared operable on March 13, 1990, it remained in a standby status for the next seven days until it was called upon during the March 20, 1990, incident. Emergency diesel generator 1B was tagged out of service on March 14, 1990, to begin its outage work, similar to that performed on emergency diesel generator 1A.

2 EMERGENCY DIESEL GENERATOR 1A POST-INCIDENT REVIEW AND TROUBLESHOOTING

Emergency diesel generator 1A was started three more times on March 20, 1990, after it had been declared inoperable. The first of these starts occurred approximately 8 hours after it was shut down from its final run during the incident. The damage to the 230-kV ac Phase C line feeding reserve auxiliary transformer 1A had been repaired at this point. The purpose for the start was to parallel the emergency diesel generator with the offsite power feed to safety bus 1A from reserve auxiliary transformer 1B so that power would remain available to train A equipment (e.g., cooling water systems, RHR system, etc.) when the offsite feed was transferred from reserve auxiliary transformer 1B back to reserve auxiliary transformer 1A. The diesel generator was manually started and tied to its safety bus. The offsite power feeder breaker to the bus was then racked out of the cubicle aligned with reserve auxiliary transformer 1B and racked into the cubicle aligned with reserve auxiliary transformer 1A. It is standard operating practice to parallel the emergency diesel generator in this manner when returning a safety-related 4.16-kV ac bus from its preferred alternate offsite power source to its normal offsite source. The diesel generator was run for 47 minutes.

The last two starts were made to see if the behavior of the emergency diesel generator during the incident (i.e., engine trip after starting) would repeat itself while the emergency diesel generator was being monitored by the licensee's engineering staff and vendor (Cooper Industries) personnel. All three of the starts after the incident were manual starts from the control room. These are received as normal start signals (as opposed to emergency start signals) by the emergency diesel generator engine control circuits, as is the LOOP start signal generated by the load sequencer. The emergency diesel generator response is the same to both signals; all engine protective trip functions remain active. The duration of the engine runs on the last two starts were 5 minutes and 21 minutes. The emergency diesel generator operated without any problems or engine trip signal alarms. The differences between the last three starts on March 20, 1990, and the LOOP signal starts during the incident were that the load sequencer did not operate, and, for the last two starts, the emergency diesel generator was operated at no-load conditions. The sequencer played a minimal role on the second start during the incident in that the control switches for several of the larger sequenced loads had been placed in the pull-to-lock position.

The licensee's root cause investigation concerning the behavior of emergency diesel generator 1A during the incident focused on two areas: (1) determination of the root causes for the unexpected trips, and (2) fully understanding the conditions necessary for restart following a trip. Even though an undervoltage condition existed on safety bus 1A following each trip, the emergency diesel generator control circuits had "locked up" in a manner that prevented subsequent restart attempts. It is not clear that this lockout condition was expected by the operators. There appeared to be confusion as to whether the lockouts were the result of equipment malfunctions or some other unrecognized condition.

The load sequencer is designed to complete its loading cycle approximately 36 seconds after the emergency diesel generator output breaker closes after a LOOP signal automatic start. During the incident, emergency diesel generator 1A supplied voltage to its safety bus for approximately 80 seconds before the first trip, and 70 seconds before the second trip. Therefore, the licensee believes that the load sequencer properly completed its cycle each time, and then reset itself as designed.

Shutdown of the emergency diesel generator is accomplished by supplying 60 psig air pressure from the engine control panel to the engine to engage the shutdown cylinder. The shutdown cylinder extends the fuel racks to shut off the fuel supply to the engine. Shutdown of the emergency diesel generator following a normal start (such as an automatic start on undervoltage at 4.16-kV ac safety bus 1A) will occur in response to either a manual stop signal or an automatic trip signal (e.g., from the engine-mounted pneumatic sensors used to protect the diesel generator). Following a shutdown, engine restart will be prevented for approximately two minutes. Time delay elements in the pneumatic control logic will maintain air pressure to the shutdown cylinder for two minutes to ensure a complete coastdown of the engine to protect against inadvertent restarts and to permit control system relays and timers to reset. Complete coastdown takes approximately one minute. The emergency diesel generator will not respond to a normal start signal received within the two-minute interval because the fuel supply to the engine is locked out. However, following the two-minute interval, restart might be expected if a normal start signal exists at that time.

Receipt of a normal start signal when the emergency diesel generator is in its standby mode causes the air start valve solenoids to energize (for a period of up to 5 seconds, or until engine speed reaches 200 rpm, whichever comes first) to admit starting air to the engine. An interlock in the starting circuit prevents energization of the air start valve solenoids whenever engine speed is in excess of 200 rpm. Following each emergency diesel generator trip during the incident, the resulting undervoltage condition at the safety bus was sensed by the load sequencer, which in turn generated another normal start signal. The signal was received by the emergency diesel generator start circuits at the engine control panel immediately following each trip. Because it takes the engine approximately 25 seconds to coast down to 200 rpm following a trip and because the 5-second interval had elapsed, the air start valve solenoids were not energized (a start during this interval is not possible because the engine fuel supply is locked out). The bus undervoltage condition remained, and the load sequencer continued to send the LOOP automatic start signal to the emergency diesel generator. As long as the load sequencer continues to provide a start signal to the emergency diesel generator, the 5-second time delay relay used to deenergize the air start valve solenoids after a normal start remains in an energized state. This prevents energization of the air start valve solenoids even after the two-minute fuel lockout has ended. The start signal must be removed to allow the time delay relay to reset, which allows a subsequent normal start attempt. Therefore, following the two diesel generator trips during the incident, the emergency diesel generator could not have been restarted by normal means, including the start pushbutton switch in the control room.

The load sequencer design includes an input memory latch circuit that locks the undervoltage signal into the sequencer until the sequencer completes its entire cycle. Therefore, the start signal transmitted from the sequencer to the emergency diesel generator also remains energized until the sequencer completes its cycle. The load sequencer can only complete its cycle if the emergency diesel generator successfully starts and picks up the appropriate safety loads. A simplified diagram of the emergency diesel generator start logic is provided in Figure J.1. The reasons for the emergency diesel generator lockouts during the incident and the conditions necessary for restart, can be summarized as follows:

- The emergency diesel generator trips resulted in bus undervoltage. The diesel generator cannot restart for two minutes because the engine fuel supply is locked out.

- Following each trip, the sequencer immediately sent a normal start signal to the emergency diesel generator control circuits, starting the 5-second timer.

- Upon completion of the 5-second interval, the timer circuit will seal in which disables the normal start circuit until the start signal is removed (removing the start signal deenergizes the timer circuit allowing it to reset).

- Because the undervoltage condition remained, the normal start signal was maintained by the load sequencer.

- The continuous start signal from the sequencer to the 5-second timer circuit created a lockout condition, preventing the emergency diesel generator from starting although engine speed had decreased to below 200 rpm and the engine fuel supply was made available.

- During the incident, the start signal was removed after the first trip by downpowering the sequencer. Restoring power to the sequencer caused it to generate another automatic start signal after the time delay circuit had reset, allowing the emergency diesel generator to restart.

From the investigation, the Team concludes that no equipment failures or malfunctions were involved with restarting emergency diesel generator 1A after it had tripped during the incident. The lockouts were the result of the way in which the load sequencer logic and the emergency diesel generator control system starting logic interact, given the sequence of events that occurred. Had the sequencer been reset following the second trip, it appears that the emergency diesel generator would have restarted as it did when the sequencer was reset following the first trip (assuming that engine speed was less than 200 rpm and that the two-minute fuel lockout period had expired). Given the design of the load sequencer and the emergency diesel generator starting circuitry, a lockout condition where the diesel generator will not respond to a normal start signal is an expected response to any trip that results in an undervoltage condition at its safety-related bus. This design feature does not appear to be undesirable in that (1) following an automatic shutdown by one of the engine protective trip functions, repeated engine restarts are not permitted, thereby, potentially preventing engine damage from continued operation, and (2) engine air rolls (i.e., admission of starting air to crank the engine while its fuel supply is locked out) are prevented that could otherwise deplete the starting air supply. At the time of the incident, it appears that the simplest way to remove the lockout condition and reset the normal start circuit was to reset the load sequencer memory latch by momentarily removing power to the sequencer.

It is noted that the first attempt to reset the load sequencer was unsuccessful. A design feature of the load sequencer is that loads which have been sequenced onto the safety bus cannot be secured by the operators until the loading cycle is complete. The last step of the loading cycle restores control of loads to the operators. A reset pushbutton switch is provided at the sequencer to allow the operators to regain control of loads for situations where power has been restored to the bus, but control of loads is not automatically restored through completion of the loading cycle. The reset switch allows the operators to secure loads that were manually sequenced onto the safety bus following a loss and restoration of offsite power where the emergency diesel generator is out of service. The operator at the sequencer first attempted to restart the emergency diesel generator by using this reset switch. The reset attempt had no effect because power was not available to the bus (the switch is not designed to interrupt the start signal from the load sequencer to the emergency diesel generator when an undervoltage condition exists on the safety bus).

If the emergency diesel generator should trip during the loading cycle, the loads that were sequenced before the trip will remain connected to the bus. The load sequencer must be manually reset to shed the loads. The licensee has determined that if the diesel generator is manually restarted and its output breaker is closed without first resetting the sequencer, the normal (nonsequenced) loads and all loads sequenced before the trip will be block loaded, potentially causing another trip. The licensee is revising their procedures to require that the load sequencer is reset before restarting the emergency diesel generator for this situation. The Vogtle plant response to Institute for Nuclear Power Operations recommendations concerning a similar design problem is discussed in Section 3.1 of Appendix E of this report.

The emergency diesel generator lockout condition occurred in response to a continuous normal start signal that was applied to the emergency diesel generator control circuits during the two-minute interval where fuel to the engine is locked out after shutdown. The LOOP undervoltage start signal was the only automatic normal start signal. The other normal start signals are momentary signals that are manually initiated from pushbutton switches. The signals will self-reset when the corresponding switch is released. However, if the switch is depressed and held for longer than 5 seconds during the two-minute interval, where fuel flow to the engine is blocked, then a normal start lockout would occur.

An emergency start signal (i.e., local manual breakglass start or safety injection signal start) will start the emergency diesel generator even if the normal start lockout condition exists. A lockout condition did exist when the breakglass start was made during the incident. An emergency start signal will instantly release the shutdown cylinder to reestablish the engine fuel supply and the air start valve solenoids will energize to provide starting air to the engine if the starting air pressure is greater than 150 psig and if engine speed is less than 200 rpm. The same sensors and relays are used to terminate the starting air supply to the engine when engine speed reaches 200 rpm for both normal and emergency starts. The 150 psig interlock prevents bleeddown of the starting air supply because of continued air rolling should the engine fail to start. This allows an opportunity to find and correct the cause for failure to start while preserving sufficient starting air pressure to attempt subsequent starts. The engine will not start if starting air pressure falls below approximately 90 psig.

Following the incident, the licensee modified the emergency diesel generator start circuitry to make the LOOP start signal from the load sequencer an emergency start signal. Therefore, the majority of the engine shutdown parameters will be bypassed, minimizing the possibility of a trip. Only the four critical engine shutdown parameters remain in effect: jacket water high temperature, lube oil low pressure, engine overspeed, and generator differential current. If an emergency diesel generator trip occurs following an emergency start, a subsequent start cannot be made until the EMERGENCY STOP RESET pushbutton is activated at the local engine control panel. Therefore, a trip following a LOOP automatic start will still result in a lockout condition that requires local reset before making another start attempt. The engine will restart upon reset if (1) an emergency start signal still exists, (2) the engine speed and starting air pressure permissive conditions are satisfied, and (3) the condition causing the trip has cleared or the trip was caused by jacket water high temperature or lube oil low pressure in which case the trip signal would be bypassed upon reset even if the trip condition still exists. Therefore, the EMERGENCY STOP RESET feature allows the operators to override the pneumatic sensors that remain capable of causing an emergency diesel generator trip following an emergency start. The modification to change the LOOP emergency diesel generator automatic start from a normal start to an emergency start was not reviewed by the Team.

It should be noted that the emergency diesel generator control system design includes a RESET FROM LOCA pushbutton switch on the engine control panel that can be used to reinstate the bypassed protective trip functions while the engine is running following an emergency start. A RESET FROM LOCA essentially reverts an emergency start signal to a normal start signal. The engine will trip upon reset if one of the previously bypassed trip conditions exists.

3 TROUBLESHOOTING FOR ROOT CAUSE OF EMERGENCY DIESEL GENERATOR TRIPS

The licensee's root cause investigation concerning the two emergency diesel generator trips that occurred during the incident was made more difficult because of the lack of data. Neither the plant computer (PROTEUS) nor the emergency response facility (ERF) computer record pretrip or trip conditions sensed by the engine-mounted sensors that automatically trip the emergency diesel generator under abnormal operating conditions. Emergency diesel generator alarms and the times at which they occur are not printed, logged, or stored for post-event analysis. Much of the information that determined troubleshooting activities was gained after the incident through conversations between system engineers responsible for the emergency diesel generators and operations personnel involved with the incident.

Some information concerning emergency diesel generator performance was documented during the incident. The operators are trained to record start and stop times, the reasons for starts, and the causes for trips in the unit shift supervisor's or unit control log book. GPC Procedure No. 13145-1, "Diesel Generators," contains a "Completion Sheet" that is filled out with information concerning each start, including the reasons for a trip or failure to start. The completion sheets are given to the emergency diesel generator system engineer. However, for unplanned starts such as those during the incident, the completion sheets are filled out afterwards, largely from information documented in the logs. It does not seem appropriate to expect the control room operators to log the emergency diesel generator performance information necessary to determine an optimum troubleshooting approach while responding to plant transients such as the loss of all power to the safety related 4.16-kV ac buses during mid-loop operation. Much of the information logged is based on observation of the local and remote emergency diesel generator annunciator panels. Although operations personnel remember that many alarms were received on the first trip during the incident, no one could remember the specific alarms. The capability to automatically record trip alarms to allow post-incident reconstruction of alarm sequences would appear desirable given the complexity of the emergency diesel generator control system and the number of alarms received on starts and trips.

Emergency diesel generator operating data is recorded whenever the engine is operated longer than 10 minutes in accordance with GPC Procedure No. 11885-C, "Diesel Generator Operation Log." The procedure identifies acceptable ranges for engine operating parameters and includes a comments section for recording abnormal conditions and corrective actions. Readings are normally taken every hour. Readings were taken every half-hour during the incident after the emergency start. The readings taken during the incident and for the three additional starts on March 20, 1990, after the incident showed normal operating conditions with all parameters within acceptable ranges.

Data available after the incident from which to develop a troubleshooting plan to determine the root causes for the trips primarily consisted of--

1. The length of time that emergency diesel generator 1A supplied voltage to safety bus 1A. Voltage at the 4.16-kV ac buses is monitored by the ERF computer, and by a Sangamo fault recorder that records multiple electrical system parameters (primarily substation and switchyard data) for fault analysis. Both sources show that voltage was supplied to the bus for 80 seconds before the first trip and for 70 seconds before the second trip, and

2. The three alarmed trip conditions that were observed by at least two operations personnel on the second trip:

   - DG1A TRIP LOW PRESSURE JACKET WATER

   - DG1A TRIP HIGH TEMPERATURE JACKET WATER

   - DG1A TRIP LOW PRESSURE TURBOCHARGER OIL

The licensee's initial troubleshooting effort focused on (1) the engine-mounted pneumatic sensors that initiate emergency diesel generator trip on jacket water low pressure, jacket water high temperature, and turbocharger oil low pressure, (2) the air lines that connect the sensors with the pneumatic logic inside the local engine control panel, and (3) the logic that actuates the engine shutdown cylinder when the sensors are tripped. The pneumatic sensing lines associated with the protective trip functions listed in item (1) are normally vented when the engine is shut down and in its standby mode. When the engine starts, 60 psig control air pressure is admitted to fill and pressurize the lines. The lines remain pressurized during operation as long as the monitored parameters remain within normal ranges. When a parameter value exceeds the setpoint for sensor actuation, the sensor will vent off the 60 psig pressure in the sensing line, causing the logic to detect a condition that requires engine shutdown. The logic in turn will supply 60 psig control air pressure to the engine-mounted shutdown cylinder to shut off the engine fuel supply. The logic is designed to prevent the sensors from causing an unwanted trip during the first 60 seconds after a start. The 60-second interval is sufficient to allow the engine-driven lube oil and jacket water system pumps to establish normal operating pressures, causing the associated sensors to seal off their vent ports and allow the sensing line pressures to reach equilibrium values. The 60-second time delay is achieved pneumatically by filling a cylinder through a .006 orifice with 60 psig control air. This portion of the pneumatic logic is referred to as the shutdown bypass timer. If a trip condition exists at the end of the 60-second interval, the logic will automatically initiate shutdown of the diesel generator. A time delay relay is used to bypass the emergency diesel generator trip alarms during the 60-second interval to prevent nuisance alarms that would occur when the engine is first starting. It is noted that the temperature alarms that are routinely received on a start originate from thermocouples that are not part of the pneumatic control system and are not bypassed.

One possible explanation for the emergency diesel generator trips during the incident was that a trip condition, either valid or perhaps caused by sensor malfunction, may have existed when the shutdown bypass timer completed its cycle. Because sensor actuation involves venting the sensor's air supply line, it was thought that a significant air leak in the sensors or sensing lines associated with jacket water low pressure, jacket water high temperature or turbocharger low oil pressure could have been interpreted by the logic as valid sensor actuation. It was thought that air leaks might also explain the difference in the length of time that the diesel generator supplied voltage to its bus during the incident (80 seconds before the first trip and 70 seconds before the second trip). The emergency diesel generator was idle for 7 days prior to the incident. If leaks existed, it was thought that more time might be required to pressurize the pneumatic system on the first start because the system would have been completely vented. Less time might have been required on the second start because system pressure may not have vented off completely after the first start. Although a difference in the time required to pressurize the system would be expected, it was thought that the time might be significantly increased because of leaks. It was also speculated that the shutdown bypass timer delay time (although fixed by passive components assuming a constant 60 psig air pressure) might be longer than 60 seconds. Note that the actual run times during the incident include the time required for the diesel generator to achieve rated speed and voltage and for the output breaker to close (approximately 7 seconds), in addition to the 80- and 70-second intervals that voltage was supplied to the bus. The first test performed by the licensee was to determine if leaks existed in the pneumatic system.

On March 23, 1990, emergency diesel generator 1A was started for the first time since the incident in order to pressurize the pneumatic system to perform leak testing. The testing involved application of a soapy solution (called "snoop" that does not leave a film residue when it dries) to air line fittings and watching for bubbles that form at leak locations. The solution was applied to fittings in the engine control panel at the bulkhead where the sensing lines leave the panel to go to the engine-mounted sensors. The solution was not applied to air line connections at the sensors or to the sensor vents to detect if leakage existed at these locations. The emergency diesel generator pneumatic trip circuitry is shown in Figures J.4 and J.5. Leaks were found in 12 of the pneumatic lines. The 12 lines included the 5 lines associated with the sensors that provided the alarms seen following the second trip (i.e., jacket water low pressure - 1 line, jacket water high temperature - 3 lines—3 sensors are arranged in a 2-out-of-3 trip logic, and turbocharger oil low pressure - 1 line; a common line is provided for the two turbochargers, and either of two sensors will initiate a trip). The fittings were tightened and repaired as the leaks were found. The magnitude of the leaks, and, therefore, the combined effect of the leaks is not known. The diesel generator was operated for 1 hour and 56 minutes during this test. Engine operation was normal with no trip or other abnormal alarms.

On March 23, 1990, the licensee also calibrated the three engine lube oil pressure sensors. The sensors are also arranged in a 2-out-of-3 trip logic and remain active following an emergency start (similar to the jacket water high temperature trip function). The sensors are manufactured by Calcon. Although no one remembers seeing a lube oil low pressure alarm on the first or second trips during the incident, a lube oil sensor malfunction alarm was received following the emergency start. Two of the three sensors (1PSL-4749B and C) calibrated satisfactorily. However, the third sensor (1PSL-4749A) would not reset. If the sensor had been venting during the incident it would explain the sensor malfunction alarm received after the emergency start. In addition, the sensing lines for lube oil pressure, jacket water pressure, jacket water temperature, and turbocharger oil pressure are supplied from the same portion of the pneumatic logic during the 60-second shutdown bypass interval following an emergency diesel generator start. It was thought that a venting lube oil pressure sensor may have prevented the other pneumatic sensing lines from becoming pressurized. This would result in a diesel generator trip and the trip alarms when the 60-second shutdown bypass and alarm bypass timers expired. The air supply lines for the other pneumatic trip sensors are either pressurized from a different portion of the logic, or the trip condition does not exist when the diesel generator is in the standby mode (i.e., the sensors are not vented when the engine is at rest). Although a jacket water high temperature condition does not exist when the diesel generator is idle, the associated air lines are more closely coupled with the lube oil pressure air lines. The licensee suspected that a venting lube oil pressure sensor or intermittent problems with the jacket water temperature sensors could have caused the emergency diesel generator trips.

Additional leaks associated with 6 pneumatic lines were discovered during functional testing of the pneumatic logic on March 29, 1990. The 6 lines included the jacket water pressure sensor air supply line, one of the jacket water temperature sensor air lines, and the turbocharger oil pressure air line that were discovered to have leaks during the snoop testing. The leaks found on March 29, 1990, were considered by vendor representatives involved with the testing to be insignificant and to not have any impact on system operation. A continuous makeup air supply is provided through an orifice to most of the sensor air lines between the pneumatic logic shutdown board and the sensor. The air supply will make up for leaks below .006 in size, but will not impact sensor venting on an actual trip. This allows small leaks to be accommodated without affecting system operation. It was concluded that the orificed air supplies to the sensors could accommodate multiple small tubing leaks and prevent trips. A .006 leak is considered large for this system. The system is designed to accommodate the venting of multiple sensors without impacting the overall sensor air supply.

It is difficult to analyze the combined effects of the multiple air leaks that existed during the incident and the lube oil pressure sensor that may have been venting at that time. The consensus between the licensee and the vendor is that it is unlikely that the leaks by themselves were the sole cause for the trips during the incident. The specific effects of the leaks cannot be determined given the complexity and interdependencies between different portions of the pneumatic logic system and the unknowns concerning leak sizes at various locations and the degree to which the lube oil pressure sensor may have been venting. It appears doubtful in the absence of additional problems (e.g., intermittent operation of a sensor or logic device) that the leaks could have caused the diesel generator to trip twice during the event given that it started and operated successfully the next four times before the system was altered. A two-day interval existed between the last two starts, which provided additional time for the pneumatic logic system to depressurize. The licensee has not ruled out the possibility that differences in the time required to pressurize the logic on the first two starts because of the leaks may have partially accounted for the 10-second difference in the times before the diesel generator tripped (80 seconds versus 70 seconds).

The next start of emergency diesel generator 1A was an inadvertent start later on March 23, 1990. It was started by mistake in lieu of emergency diesel generator 1B, which was to have been started as part of a post maintenance functional test. Emergency diesel generator 1A was shut down within a minute and its performance was not closely monitored during this brief run. The next start of emergency diesel generator 1A would not be until 6 days later on March 29, 1990.

After concluding that the leaks identified in the emergency diesel generator's pneumatic control system could not have by themselves caused the trips during the incident, the licensee focused their root cause investigation on the pneumatic logic and the engine-mounted pneumatic sensors. A test sequence was developed to determine whether the engine control system pneumatic logic circuits used to start and automatically trip the emergency diesel generator were functioning properly. In a parallel effort, the licensee began investigating the sensors used to trip the diesel generator on jacket water low pressure, jacket water high temperature, engine lube oil low pressure, and turbocharger oil low pressure. A discussion of the scope and results of the tests follows.

3.1 Control System Functional Testing

The troubleshooting planned by the licensee to determine the root cause for the trips during the incident included a series of tests of the engine control system. The tests were (1) designed to recreate the sequence of events that occurred during the incident while the emergency diesel generator was being closely monitored and (2) to demonstrate proper functioning of the individual pneumatic elements that collectively make up the emergency diesel generator automatic shutdown logic. A leak test was performed for the pneumatic sensing lines, and a multiple start test was performed to verify operability of the control system after the logic functional test, which involved breaking and subsequently restoring both pneumatic and electric circuits. An undervoltage condition on safety bus 1A (as sensed by the load sequencer during the event) was created to verify proper emergency diesel generator response and that the troubleshooting activities had not introduced or recreated the trip problems experienced during the incident. Lastly, the 6-month operability testing required by the plant technical specifications was performed to confirm operability of the emergency diesel generator. The licensee believed that this series of tests, combined with the planned sensor testing, provided a comprehensive troubleshooting plan for root-cause determination that encompassed all suspect equipment involved during the incident. Each of the tests and the results achieved are addressed below in the order in which the tests were performed.

Undervoltage Test No. 1: The first of two undervoltage tests was performed on March 29, 1990. The purpose of the test was to simulate as closely as possible the LOOP condition that resulted in the automatic start of emergency diesel generator 1A on March 20, 1990. Before the test, three video cameras were installed to record the response of (1) annunciators and gauges at the local engine control panel, (2) meters and indications on the generator control panel, and (3) additional gauges mounted at the emergency diesel generator skid. The offsite power feeder breaker supplying 4.16-kV ac safety bus 1A was tripped, creating an undervoltage condition. The licensee verified that the load sequencer automatically shed bus loads and provided an automatic start signal to emergency diesel generator 1A; that the diesel generator started, achieved rated speed, voltage, and frequency; that the output breaker closed restoring power to the bus within an acceptable time; and that bus loads were automatically sequenced as designed. The diesel generator was operated for approximately 16 minutes before being manually stopped. The diesel generator operated satisfactorily without abnormal conditions or trip alarms. Starting air low pressure and generator underfrequency alarms were received when the diesel generator started. A third alarm, low temperature lube oil-in was received a short time later. Only the starting air low pressure alarm remained after acknowledge and reset of the annunciator.

Engine Control Panel Functional Test: The purpose of the engine control panel functional test is to verify proper operation of the individual logic functions performed by the pneumatic control system. The test verifies proper system response to actuation of control inputs (e.g., starts, stops and resets), proper alarm and status light indications, proper response to simulated trip conditions, proper operation of the engine shutdown cylinder, approximate timing of system delay times (e.g., shutdown bypass timer), and that system pressures are appropriate under various conditions. The test is not intended to verify proper calibration of devices in the panel (e.g., that a pneumatic pressure switch actuates at 45 psig and resets at 40 psig). The test also verifies operation of the electrical portion of the engine control system. Post-incident troubleshooting was concentrated on the pneumatic portion since the test had been recently performed during the outage, and it was believed that any problems that could explain the emergency diesel generator trips would be found in the pneumatic portion of the system. All pneumatic logic circuits tested satisfactory. The test was revised to include specific timing of the shutdown bypass time delay interval. The interval was checked three times and was measured to be 63 seconds twice and 65 seconds once. These results showed that the shutdown bypass timer was relatively consistent as expected, but that the time could vary slightly. It is noted that the engine control panel functional test is a relatively new test performed by the vendor. The test had been performed six times before the incident (twice for both the 1A and 1B emergency diesel generators at Vogtle, and once for each emergency diesel generator at River Bend).

Bubble Leak Test: Leak testing was performed in two phases. The first phase consisted of bubble testing. The emergency diesel generator was started via an emergency start signal to prevent it from tripping when individual pneumatic sensing lines were disconnected during the test. A bubble tester is connected in series with the 60 psig air supply to the sensing line being tested. Once the tester is connected and the line has repressurized, the air supply to the sensor is rerouted through a water filled sight glass. Any leaks in the sensing line downstream of the engine control panel or at the sensor are revealed by air bubbles flowing from the supply through the water to the leak location. After the test, the tester is removed and the air line that was broken to install the tester is reconnected. The second phase of leak testing involves application of snoop leak-detector solution to the reconnected air line fittings to verify they are tight and not leaking. The leak testing was performed on March 30 and March 31, 1990.

Twelve pneumatic sensing lines are provided for the emergency diesel generator trip parameters listed in Table 3.1. The lines associated with the three jacket water temperature sensors were the last to be tested. A jacket water temperature sensor malfunction alarm was received when the emergency diesel generator was started, indicating that one of the sensors may be venting. When the first of the three lines was disconnected to install the bubble tester, the emergency diesel generator tripped. A trip is normally an unexpected response because the jacket water high temperature trip function uses a 2-out-of-3 logic; venting a single sensing line should not cause a trip. The trip confirmed that a problem existed in one of the other sensing lines or sensors. For troubleshooting purposes, gauges were installed in the three sensing lines to monitor the air pressure at the sensor inputs, and the diesel generator was restarted. Restart of the diesel generator with all lines connected revealed that one sensor was venting (sensor ITSH-19111) and that another sensor (ITSH-19112) was leaking. The venting sensor was correctly sensed by the logic as a trip condition. Disconnecting the sensing line to install the bubble tester had caused a second line to be vented, which satisfied the trip logic and resulted in the trip. The air line to the venting sensor was crimped, to allow air pressure to build, and subsequently released to pulse the sensor with air pressure. This sequence was repeated several times, causing the venting sensor to reset, sealing off its vent port, and allowing its sensing line to repressurize. Sensors ITSH-19111 and ITSH-19112 were quarantined by the Team and were replaced later on March 31, 1990. The leak testing on the jacket water temperature sensing lines was completed after the new sensors had been installed. All three jacket water temperature sensors had been recalibrated earlier on March 30, 1990, (before the leak testing) as part of a temperature sensor recalibration effort initiated because of inconsistencies found in previous calibrations. The licensee's investigation of temperature sensor calibration and performance is addressed later in this section. Except for the temperature sensors, no significant leaks were identified during the leak testing.

Multiple Start Test: The purpose of the multiple start test was to verify proper overall integrated performance of the pneumatic and electric portions of the engine control system. The engine control panel functional test, which involved breaking electrical connections (e.g., opening sliding links to prevent energization of the air start solenoids) as well as disconnecting pneumatic lines, exercised the individual portions of the emergency diesel generator control logic, but did not start the engine. The emergency diesel generator six-month operability test to be performed as the final test in the troubleshooting sequence only requires a normal start signal, followed by a normal stop signal upon completing of the test. The multiple start test was designed to verify proper emergency diesel generator response to various start signals (i.e., normal and emergency starts) and various stop signals (i.e., trip signals initiated by venting pneumatic lines associated with sensors that are pressurized from different portions of the shutdown logic). This combination of tests is a more integrated approach to demonstrate overall operability of the emergency diesel generator engine control system. The test was performed on March 30 and March 31, 1990. Video cameras were again used to monitor the local annunciator panel and gauges as during the undervoltage test. The test involved four sets of emergency diesel generator starts and stops. The test results were satisfactory. There were no unexpected operating conditions, problems or trip alarms. The start and stop signals and the alarms received on each trip are listed below:

Test No. 1: Start signal: manual normal start
Stop signal: lube oil high temperature
Trip alarms: high temperature lube oil trip,
generator underfrequency,
high temperature lube oil-in, and
high temperature jacket water-out

Test No. 2: Start signal: simulated loss of offsite power automatic normal start
Stop signal: high vibration
Trip alarms: high vibration trip,
high temperature lube oil-in,
generator underfrequency, and
high temperature jacket water-in

Test No. 3: Start signal: manual normal start
Stop signal: crankcase high pressure
Trip alarms: crankcase high pressure trip, and
generator underfrequency

Test No. 4: Start signal: simulated safety injection signal automatic
emergency start
Stop signal: lube oil low pressure
Trip alarms: unknown; not recorded

Note that several spurious temperature alarms were received on two of the trips during the multiple start test. The temperature alarms were also received during other post-incident troubleshooting tests and have been common on many emergency diesel generator starts at Vogtle. The alarms are actuated from action-pack relays that receive millivolt signals from thermocouples used to sense jacket water and lube oil system temperatures. The relays are sensitive to voltage perturbations, by design, and appear to be spuriously actuated by voltage spikes induced by other valid alarm signals. Spurious alarms were also observed on other starts during testing (e.g., starting air low pressure). The Team observes that multiple unnecessary alarms may have been confusing or annoying to the operators and that reset of the annunciator panels in an attempt to clear the nuisance alarms may have resulted in the loss of valid information concerning the cause for the first emergency diesel generator trip during the incident.

At this point during troubleshooting, the licensee performed two additional tests that were not originally planned as part of the test sequence. The first test was designed to quantify the time interval between an emergency diesel generator start and emergency diesel generator trips on jacket water high temperature and jacket water low pressure. The second test was designed to determine whether actual high temperature conditions were associated with the jacket water keep-warm system that could have resulted in premature actuation of the jacket water temperature trip sensors on an emergency diesel generator start. These two additional tests are discussed below.

Emergency Diesel Generator Trip Timing Test: The purpose of this test was to determine whether a preexisting false jacket water high temperature condition, as sensed by the pneumatic logic (i.e., at least two sensing lines vented), could have caused the emergency diesel generator trips during the incident. The test involved disconnecting two of the three jacket water temperature sensing lines to intentionally simulate a high temperature trip condition before starting the diesel generator so that it would trip upon completion of the shutdown bypass timer. A recorder would be used to monitor diesel generator output voltage, and the length of time that the diesel generator supplied voltage to the bus during the test would be compared with times that bus voltage was supplied during the incident to see if they matched. Video cameras were again used to monitor the annunciator panel and local gauges. The test was performed on March 31, 1990.

An initial emergency diesel generator start was made with all sensing lines connected to ensure that there were no jacket water temperature trip or sensor malfunction alarms, or other abnormal alarm conditions that could invalidate the test. There were no abnormal alarms, and the emergency diesel generator was stopped. The alarms can only be detected with the diesel generator operating because all alarm conditions that are sensed by the pneumatic portion of the control system are normally bypassed and only become active 60 seconds after the engine has started. The alarms are bypassed to prevent nuisance alarms that would occur because the condition exists with the engine at rest or because the pneumatic system had not become fully pressurized after the engine is first started. Therefore, if a sensor is erroneously venting (e.g., a jacket water high temperature sensor in the tripped condition) with the engine at rest, it would not be detected until 60 seconds after the engine was running, at which time the shutdown bypass timer would expire, potentially causing an emergency diesel generator trip. Note that some of the pneumatic sensors are correctly venting as designed with the engine at rest (e.g., pressure sensors for engine lube oil and jacket water).

Two of the three jacket water temperature sensing lines were disconnected (line E-16A to sensor ITSH-19111, and line E-16C to sensor ITSH-19110) to simulate a trip condition. The emergency diesel generator was started, using the normal manual start switch in the control room. The start switch contacts are in parallel with the contacts that provided the loss of offsite power normal start signal from the load sequencer during the incident. The diesel generator automatically tripped as expected at the end of the shutdown bypass time interval. This test was repeated two more times; once with the same two sensing lines vented, and once with lines E-16B (to sensor ITSH-19112) and E-16C vented (line E-16A was reconnected). The results for all three trips were identical. The same seven alarms were received after each trip, and, with one minor exception, the alarms were received in the same order each time. The alarms included the three alarms seen by the PEOs at emergency diesel generator 1A following the second trip during the incident (i.e., DG1A TRIP LOW PRESSURE JACKET WATER, DG1A TRIP HIGH TEMPERATURE JACKET WATER, and DG1A TRIP LOW PRESSURE TURBOCHARGER OIL). The seven alarms are listed below in the order in which they were received during the tests:

- DG1A TRIP LOW PRESSURE JACKET WATER
- DG1A TRIP LOW PRESSURE TURBOCHARGER OIL
- DG1A HIGH TEMPERATURE LUBE OIL-IN
- DG1A HIGH JACKET WATER TEMPERATURE SENSOR MALFUNCTION
- DG1A TRIP HIGH TEMPERATURE JACKET WATER
- DG1A HIGH TEMPERATURE JACKET WATER-IN
- DG1A GENERATOR UNDERFREQUENCY

For one of the trips, the lube oil temperature alarm came in after the sensor malfunction alarm.

Interestingly, not only did the preexisting jacket water high temperature condition result in the other trip alarms, but the jacket water low pressure and turbocharger oil low pressure trip alarms came in together approximately 10 seconds ahead of the jacket water high temperature sensor malfunction and trip alarms. Because the jacket water temperature, jacket water pressure and turbocharger oil pressure sensing lines are pressurized from a common point in the pneumatic logic during the shutdown bypass timer interval, it is possible that the two disconnected and vented lines did not allow any of the other lines to pressurize, causing the logic to falsely sense all three trip conditions. The three alarms only occur together if the jacket water temperature sensors or sensing lines are vented before the engine is started. The jacket water low pressure and turbocharger oil low pressure trip alarms will not activate if the jacket water high temperature sensing lines are vented after the diesel generator has been operating past the shutdown bypass time interval.

The licensee believes that the time from when the emergency diesel generator output voltage reaches 4.16-kV ac after a start until the voltage drops off on a trip is a good approximation (i.e., within approximately 1 second) of the time that the emergency diesel generator would supply voltage to its bus because the closing and tripping of the output breaker closely follows these times. The time from when voltage reached 4.16-kV ac until it dropped off from 4.16-kV ac was measured to be 65.6 to 66 seconds for each of the three tests. This time differs from the 80-second and 70-second intervals that voltage was supplied to safety bus 1A from emergency diesel generator 1A during the incident. It is not clear how meaningful this data is since the pneumatic system had been altered since the event. Specifically, (1) two of the jacket water temperature sensors had been replaced, (2) all three lube oil pressure sensors had been replaced, one of which was found to be venting during subsequent calibration and may have been venting during the incident, and (3) a number of leaks throughout the system had been repaired.

For the next part of the test, the jacket water pressure sensing line was disconnected (after the jacket water temperature sensing lines had been reconnected) and the emergency diesel generator was started as before to determine the time that the emergency diesel generator would have supplied bus voltage before a trip and the alarm conditions received on the trip. The time that bus voltage would be supplied was measured to be 70.5 seconds. Again, the usefulness of this data is not clear since the pneumatic control system had been altered after the incident. The alarms received on the trip are listed below in the order in which they occurred:

- DG1A TRIP LOW PRESSURE JACKET WATER
- DG1A TRIP LOW PRESSURE TURBOCHARGER OIL
- DG1A GENERATOR UNDERFREQUENCY
- DG1A HIGH TEMPERATURE LUBE OIL-IN

The licensee believes that the significance of the test results is that a preexisting jacket water low pressure trip condition will not cause a jacket water high temperature trip or sensor malfunction alarm. Because the preexisting jacket water temperature trip condition did cause the jacket water low pressure and turbocharger oil low pressure alarms, the licensee believes that the second trip during the incident was probably caused by a high jacket water temperature condition as sensed by the pneumatic logic. After the incident, the licensee recalibrated the jacket water low pressure and turbocharger oil low pressure trip sensors for emergency diesel generator 1A. The sensors were found to be in proper calibration with no adjustments necessary and were returned to service. It appears impossible to determine the degree to which the pneumatic control system leaks that existed during the incident, and which may have included a venting lube oil pressure sensor, contributed to the cause for the trips or the difference in the times that the emergency diesel generator supplied bus voltage before the trips.

A jacket water high temperature trip condition will also cause the emergency diesel generator to trip following an emergency start. During the incident, there was no jacket water temperature sensor malfunction alarm following the emergency start. This implies that if the second trip was solely caused by the pneumatic logic sensing a high jacket water temperature condition, then either (1) an actual high temperature condition existed (as sensed by at least two of the three sensors) and cleared itself by the time of the emergency start or (2) at least two of the jacket water temperature sensors or some other portion of the pneumatic logic may have been behaving intermittently or erratically. If the latter, it is fortunate that the condition cleared itself before the emergency start. Although, an existing jacket water high temperature emergency diesel generator trip condition can be bypassed using the EMERGENCY STOP RESET pushbutton switch, it is not clear that use of the switch was fully understood by the operators. Jacket water high temperature is not retained as an emergency trip signal at all plants.

Jacket Water Temperature Test: The purpose of this test was to determine whether actual jacket water temperature at the sensors could have been high enough to cause a valid trip. The sensors are located in the jacket water return header at the top of the engine as shown in Figure 3.7. The instrumentation and control (I&C) technicians that calibrate the sensors had observed that the sensor setpoint tended to decrease (i.e., the sensor would vent at a lower value) when the sensor was exposed to sudden temperature increases. Because the jacket water system contains a water tank that is heated and because the engine driven water pump is much larger than the keep-warm system pump (1600 gpm vs 90 gpm), it was theorized that a slug of hot water could be circulated to the sensors when the diesel generator is started, causing sensor actuation and unwanted trips. Before the test, one of the three jacket water temperature trip sensors was removed and a thermocouple was installed in its place. The engine was kept idle for 24 hours while the temperature was monitored. The temperature remained constant between 161 °F and 163 °F throughout this period. The tank heater is set to come on at approximately 150 °F, and shut off at approximately 170 °F. The heater was energized for most of the 24-hour period.

The test was designed to duplicate emergency diesel generator operation and jacket water temperature conditions as they occurred during the incident. The engine was started and operated for 87 seconds, stopped, started again 19 minutes later and operated for 77 seconds, stopped again, and restarted for the final time and allowed to run 35 minutes after the initial start. The engine was not air-rolled before the starts to ensure that jacket water system temperatures were not altered because of mixing. The tests results showed that jacket water temperature actually decreased to approximately 155 °F within 30 seconds after the first start and remained within several degrees of this value throughout the test. The lower temperature is attributed to NSCW flow to the jacket water heat exchangers. A temperature control valve that operates to throttle NSCW to the heat exchanger fully opens at a jacket water temperature of 170 °F and fully closes at 150 °F. Based on the test results, the licensee concluded that the actual jacket water temperature during the incident was never higher than approximately 155 °F, except for a few seconds after the initial start, and that there were no drastic temperature changes at the sensors. Following an emergency diesel generator start, jacket water temperature changes very little. The operations personnel that arrived in the emergency diesel generator room after the first start during the incident confirmed that jacket water temperature was within its normal range during the subsequent starts.

Based on the test results to date, the licensee believed that the most probable root cause for the emergency diesel generator trips during the incident involved intermittent operation of the Calcon jacket water temperature sensors, causing the pneumatic control logic to sense a false high temperature condition.

Undervoltage Test No. 2: The second of the two undervoltage tests was performed on April 7, 1990, using the same procedure as used during the first undervoltage test. Again, the diesel generator automatically started, restored power to its bus, and was loaded by the load sequencer as designed. The test was completed satisfactorily with no abnormal operating conditions or trip alarms.

Operability Test: The final test of the licensee's troubleshooting plan test sequence was the emergency diesel generator 6-month operability test used to satisfy technical specification surveillance requirements. The test involves starting the diesel generator from ambient conditions, fully loading the diesel generator (6100 and 7000 kW) in less than 60 seconds, and operating it for at least an hour in the loaded condition. The test results were again satisfactory.

At this point, the licensee had started emergency diesel generator 1A approximately 21 times since the incident with no known abnormal operating conditions or trip alarms. Following the 6-month operability test, the licensee resumed the weekly and monthly operability tests required by technical specifications. For the first two weeks, the operability test was performed three times, resulting in 6 additional starts. The diesel generator operated satisfactorily each time. On the basis of the number of successive successful starts, the licensee believes that emergency diesel generator 1A is fully operable and capable of performing its safety function.

3.2 Jacket Water Temperature Sensor Testing

The temperature sensors are manufactured by California Controls Company (Calcon). The sensor is shown in Figure 3.9. A cross-sectional diagram of the sensor is provided in Figure J.2. The same sensor (Model A3500-W3) is used to sense both jacket water and lube oil temperature. The sensor is mounted in a stainless steel thermowell and is held in place by a set screw. A combination of 1/4-inch and 3/8-inch sensing lines provide 60 psig control air from the engine pneumatic control logic to the sensor when the emergency diesel generator is running. The sensor air supply line is attached to the sensor by a stainless steel Swage-Lock fitting. The sensor is designed to block air flow when monitored temperature is below the setpoint value (200 °F ± 4 °F for both jacket water and lube oil), and to vent the air supply to atmosphere when the setpoint is exceeded.

The setpoint is adjusted to the desired value by rotating the setpoint adjustment disc mounted on the threaded end of the sensor shaft. Rotating the disc changes the clearance between the underside of the disc and the poppet valve stem. As temperature increases, thermal discs at the sensor probe expand to move the shaft downward. When temperature increases above the setpoint value, the shaft moves far enough to cause the setpoint adjustment disc to contact and push the poppet valve stem downward. This unseats the valve and allows air pressure to flow upward past the valve and escape through the sensor vent port, depressurizing the sensing line. The pneumatic logic at the engine control panel senses the depressurized air line as a trip signal. As temperature returns to below the setpoint, the thermal discs contract, allowing the return spring to move the shaft back upward. The setpoint adjustment disc will move off of the poppet valve stem, allowing the poppet spring to reseat the valve and prevent further air flow from the sensing line supply to the sensor vent. The air supply line will then repressurize if the emergency diesel generator is running.

The licensee has stated that the temperature sensors are qualified for 40 years of service. The sensors are calibrated at each refueling outage. General calibration instructions are provided in GPC Procedure No. 22332-C, "Temperature Switch Calibration." The procedure is generic to different types of temperature sensors. It contains precautions and limitations, identifies required test equipment, and provides calculation and data sheets to be completed as part of the calibration process. When completed, the data sheet identifies the specific sensor being calibrated, the expected trip setpoint and reset values (and the corresponding acceptable high and low limits), the as-found and as-left trip setpoint and reset values, and the test equipment used during the calibration and the corresponding calibration due dates. The data sheets are signed by the technician performing the calibration and reviewed, approved, and signed by the I&C Foreman. The acceptance criteria is that "the temperature switch is within limits specified on the data sheet." One of the precautions listed in the calibration procedure is to "minimize the entry of foreign materials or dirt into the working part of the instrument."

Calibration of the emergency diesel generator jacket water and lube oil high temperature pneumatic trip sensors is performed in accordance with maintenance work orders. The work orders contain additional specific calibration instructions. The sensor, installed in a thermowell, is immersed in a silicon oil bath that is heated to the trip setpoint. Air pressure to the sensor is supplied via a .028 orifice in the same manner as air is supplied from the engine control logic to the sensor during operation. In addition, the sensor is continuously tapped lightly on its side to simulate engine vibration. A sensor will typically respond during calibration by starting to vent slightly several degrees below the trip setpoint. As temperature continues to increase to the trip setpoint, the poppet valve begins to open, further reducing the pressure of the air supply. The sensor is considered tripped when supply pressure drops to 20 psig. Although individual sensors respond at somewhat different rates, sensors generally depressurize to below 20 psig within a minute. The size of the poppet valve opening appears to be at least several times larger than the .028 supply orifice. As the temperature of the bath is decreased, the sensor is considered reset when supply pressure returns to above 40 psig. The bath is required to be cooled to 20 °F below the trip setpoint before reheating to make another calibration check. The sensor is required to reset to within 1 psig of the supply pressure at 20 °F below the trip setpoint. If not, the sensor is considered failed. Setpoint adjustments are required until the setpoint is found to be within tolerance on three consecutive heatup cycles. The bath temperature is to be adjusted in smaller increments as the trip setpoint is approached, allowing temperature to stabilize after each increase. The bath heatup rate is not specified, but 1 °F per minute is used as standard practice between 180 °F and the trip setpoint. A diagram of the test arrangement used for calibration is shown in Figure J.3.

Sensor calibration appears to be somewhat dependent on the individual I&C technician performing the calibration. For example, the amount of tapping on a sensor during calibration may vary between technicians. If the trip setpoint was found within tolerance, but near its high or low limit, the technician performing the calibration would decide whether or not to attempt to adjust the setpoint closer to its expected value. For calibrations performed before the incident, it is not clear whether the sensors were transported back to the emergency diesel generators from the I&C shop in or out of a thermowell. This could be significant because the tip is the most delicate part of the sensor, and jarring it can potentially cause a 5 °F to 10 °F change in the setpoint. Twisting the tip of the sensor probe has the same effect as rotating the setpoint adjustment disc. Although the guidance provided with the maintenance work orders requires the sensors to be calibrated in a thermowell, the licensee could not confirm that all technicians used thermowells. Some test results have shown that calibration accuracy is not significantly affected by not using a thermowell. Differences in air supply pressure and bath temperature heatup rates could also have some effect on setpoint determination. The as-left setpoint values recorded on the data sheets are the average of three separate calibration checks. Some technicians record the values from all three checks on the calculation sheet and show the average value calculation. Other technicians simply record the average value on the data sheet without showing data from the individual checks. The Team found no evidence that the licensee had reviewed sensor calibration history data for identification of possible trends or failure mechanisms that could lead to reduced sensor reliability.

It appears conceivable that some combination of inconsistencies in the calibration process such as described above could result in setpoint miscalibration of several degrees. However, it seems doubtful that these factors could account for a decrease in the trip setpoint of over 35 °F (from 200 °F to below 165 °F), the difference needed to cause sensor actuations leading to the emergency diesel generator trips during the incident. The licensee requested a vendor representative to observe their sensor calibration process to determine if the calibrations had somehow contributed to the root cause for the trips. The emergency diesel generator 1A jacket water temperature sensors had all been calibrated within several weeks of the incident. The licensee indicated that the only recommendation made by the vendor was to transport the sensors in thermowells when moving them between the I&C shop and the diesel generators.

The team quarantined eight temperature sensors following the incident. All but one of the sensors were found to leak air. Two of the three jacket water temperature sensors installed on emergency diesel generator 1A during the incident (ITSH-19111 and ITSH-19112) were among the quarantined sensors. The sensors quarantined and their calibration histories are summarized below.

1. Sensor ITSH-19111, emergency diesel generator 1A jacket water temperature:

    - Installed on October 30, 1988; as-left setpoint was 197.4 °F
    - Recalibrated on January 25, 1990; as-found setpoint was 206.2 °F, as-left setpoint was 199.1 °F
    - Calibration rechecked on March 29, 1990; as-found and as-left setpoint was 198.6 °F
    - Sensor was found leaking during emergency diesel generator testing on March 30, 1990

2. Sensor ITSH-19112, emergency diesel generator 1A jacket water temperature:

    - Installed on November 19, 1989; as-left setpoint was 199.4 °F.
    - Recalibrated on March 1, 1990; as-found setpoint was 210.4 °F and as-left setpoint was 203.1 °F.
    - Calibration rechecked on March 30, 1990; as-found setpoint was 186.2 °F and as-left setpoint was 199.9 °F.
    - Sensor was found leaking during emergency diesel generator testing on March 30, 1990.

3. Sensor ITSH-19146, emergency diesel generator 1A lube oil temperature:

    - Installed on February 11, 1986; as-left setpoint was 200 °F.
    - Recalibrated on September 30, 1988; as-found and as-left setpoint was 202 °F.
    - Recalibrated on January 25, 1990; as-found setpoint was 211 °F; as-left setpoint was 200.2 °F.
    - Calibration rechecked on March 29, 1990; as-found setpoint was 190.4 °F. Sensor was behaving sluggishly and was leaking.

4. Sensor ITSH-19117, emergency diesel generator 1B jacket water temperature:

    - Installed on October 31, 1988; as-found setpoint was 199.7 °F.
    - Recalibrated on January 25, 1990; as-found and as-left setpoint was 201 °F.
    - Trip setpoint checked on March 26, 1990; as-found setpoint was 190.6 °F. Sensor was found leaking.

5. Sensor ITSH-19153, emergency diesel generator 1B lube oil temperature:

    - Installed on August 25, 1985; as-left setpoint was 200 °F.
    - Recalibrated on September 28, 1988; as-found and as-left setpoint was 199.8 °F.
    - Recalibrated on March 14, 1990; as-found setpoint was 300 °F; as-left setpoint was 199 °F.
    - Sensor would not calibrate within tolerance on March 23, 1990.

6. Sensor ITSH-19117, emergency diesel generator 1B jacket water temperature:

   - Never installed; was taken from warehouse as a replacement for sensor No. 4 above, but was found leaking on March 27, 1990, during its initial calibration.

7. Sensor ITSH-19119, emergency diesel generator 1B jacket water temperature:

   - Installed on October 26, 1988; as-left setpoint was 201.5 °F.
   - Recalibrated on January 25, 1990; as-found and as-left setpoint was 200 °F.
   - Trip setpoint checked on March 26, 1990; as-found setpoint was 188.2 °F. Sensor was found leaking.

8. Sensor ITSH-19153, emergency diesel generator 1B lube oil temperature:

   - Installed on March 23, 1990; as-left setpoint was 203.4 °F.
   - Calibration rechecked on March 27, 1990; as-found setpoint was 203.5 °F. Sensor was found leaking.

A review of the calibration history data for the emergency diesel generator 1A and emergency diesel generator 1B jacket water and lube oil temperature sensors shows that big and small setpoint drifts occurred in both the high and low directions over both long and short time intervals. The only trend identified that could potentially be relevant to sensor behavior during the incident is that five cases were found since January 1, 1990, in which the trip setpoint decreased between 9 °F and 17 °F within approximately two months of the previous calibration. In all five cases the sensor was found to be leaking air. In most cases, the leaks were small, and, in some instances, could only be detected using snoop leak-detector solution at the sensor vent port. Representatives from both the emergency diesel generator vendor and the sensor vendor have indicated that small amounts of leakage at ambient temperature would not result in unwanted emergency diesel generator trips and are not of concern as long as the trip setpoint and reset point of the sensor functioned properly. Leaks that result in less than a 1 psig decrease in air supply pressure are considered insignificant.

The licensee contracted an independent laboratory, Wyle Laboratories Scientific Services and Systems Group (Wyle) located in Huntsville Alabama, to inspect and test the quarantined sensors. The purpose of the Wyle tests was to (1) determine the causes for the observed changes in trip setpoint values between recent calibrations, (2) determine the cause for the sensors leaking, and (3) determine if these or other factors involving sensor performance could have initiated the emergency diesel generator trips that occurred during the incident. The test methodology developed by the licensee and Wyle involved a series of tests performed on two new sensors to determine their performance and response characteristics under different conditions. The new sensors would then be disassembled and inspected to allow the test engineers to become familiar with the sensor internals. The knowledge and experience gained from testing the new sensors would then be used to develop a troubleshooting test program for the quarantined sensors.

The tests and inspections performed on the two new sensors were to include (1) checks to determine if the spacer tube was loose or tight and to scribe the as-found position of the tube in relation to where it attaches to the lower body of the sensor, (2) tests to determine the as-received trip setpoints and calibration adjustments as necessary to achieve a trip setpoint of 200 °F ± 2 °F, (3) tests to determine the effects of varying heatup rates, air supply pressures, ambient temperatures and vibration levels on the sensor setpoint response, (4) the effects of in-thermowell versus out-of-thermowell calibrations on the trip setpoint, and (5) the effects of physically handling the sensor when moved in and out of the thermowells. The test configuration used by Wyle was similar to that used during sensor calibration at Vogtle, with the exceptions that additional temperature sensing elements were used to monitor the temperature of the bath, the bath medium was water versus silicon oil, and a datalogger was used to monitor air pressure and bath and in-thermowell temperatures.

Initial inspection at Wyle revealed that the spacer tube on one of the two test sensors was not secured tightly against the lower portion of the sensor body as designed, but was loose and easy to turn. The spacer tube on the other sensor appeared to be screwed tightly into the sensor body. The loose spacer tube was tightened and the trip setpoints were calibrated to 200 °F ± 2 °F. The trip setpoints of the two sensors were fairly close during initial testing, but during subsequent testing the setpoint for one of the sensors was found to be noticeably lower. Inspection of the sensor showed that the spacer tube had slightly loosened from the sensor body. The affected sensor was the one that appeared to have its spacer tube tightly secured to the sensor body during initial inspection. Finding a loose spacer tube during testing was not unexpected. On April 2, 1990, a vendor representative inspected a sensor that the licensee had recently rejected during its initial calibration because it appeared to operate sluggishly. The vendor representative found that the spacer tube had loosened from the sensor body. The spacer tube was tightened and the sensor functioned satisfactorily during subsequent testing.

The effect of the spacer tube loosening is to lower the trip setpoint. As the spacer tube loosens, the sensor shaft is pulled downward, reducing the gap between the setpoint adjustment disc and the poppet valve stem. This results in a decrease in the temperature required to cause the sensor to vent. The spacer tube is supposed to be tightly secured to the sensor body, using a thread-locking compound to prevent separation. The Wyle testing concluded that the trip setpoint decreases approximately 80 °F for each full turn of the spacer tube away from the sensor body. Several temperature sensors have been found with loose spacer tubes. A loose spacer tube would be considered a probable cause for premature sensor actuation, however, it is not clear that this type of problem could cause the intermittent behavior of the jacket water temperature sensors believed to have occurred during the incident.

In general, the temperature sensors performed well throughout the Wyle testing. Although the trip setpoint was found to change slightly from test to test, the sensors demonstrated good repeatability, consistently within several degrees of the trip setpoint. The effects of input air pressure variations of 5 psig or less (i.e., from 55 psig to 65 psig) on the trip setpoint were negligible. Vibration was found to have virtually no effect on the trip setpoint. The practice of tapping the sensor during calibration is discouraged because it is considered unnecessary and could result in the masking of internal friction problems. Although the test results confirmed that slower heatup rates tend to result in higher trip setpoints (and conversely, that faster heatup rates tend to result in lower trip setpoints), the effect of different heatup rates on the trip setpoint was relatively small. The heatup rates were varied between 1 °F per minute and 20 °F per minute during testing. A slower heatup rate allows the thermowell internal temperature to more closely follow bath temperature.

One factor that appeared to significantly affect the trip setpoint was calibrating the sensor without the use of a thermowell (i.e., with the sensor tip directly exposed to the bath). This resulted in a downward shift of approximately 10 °F in the trip setpoint. A mineral residue deposit from the water bath was found on the surface of the sensor probe. The sensors were cleaned, recalibrated, and remained in calibration during subsequent testing. The Wyle tests concluded that the sensors should be calibrated in thermowells. The Wyle testing concluded that the reference temperature used to determine the trip setpoint should be the temperature of the bath and not the temperature inside a second thermowell. This is because the air gap between the inside wall of the thermowell and the reference temperature sensing device used in the test was larger than the gap between the wall and the sensor probe. Using the bath temperature as the reference provides a more realistic setpoint because it is based on the actual temperature of the process being monitored and does not involve heat transfer delays between the process and the reference element. The testing also concluded that the sensors should be allowed to soak for at least two hours at ambient temperatures before calibration (i.e., at the jacket water and lube oil keep warm temperatures) to allow the temperature of internal components to stabilize. This would allow the internals, such as the upper portion of the shaft, to expand to positions that more closely reflect their service environment, and will result in a more accurate trip setpoint. Failure to allow proper stabilization of sensor temperatures will result in a slight upward shift of the trip setpoint. The effects of handling the sensor probe on the trip setpoint was not tested by Wyle. The vendor has indicated that the sensors should be handled with care to prevent misalignment. The testing at Wyle was closely monitored by the licensee and by the NRC.

The licensee is developing a new procedure (GPC Procedure No. 22981-C, "Calcon Pneumatic Temperature Sensor Calibration") that will provide more specific and structured guidance for sensor calibrations. The procedure will include lessons learned from the testing at Wyle and will be reviewed for comments by the vendor and plant engineering staff.

The quarantined sensors were inspected for physical damage upon receipt at Wyle. None was found. The sensors were then examined to determine if their spacer tubes had become loose from the sensor body. All spacer tubes were found tight. The spacer tube to sensor body position was scribed to determine if the alignment was retained during subsequent testing.

The sensors were next connected to 60 psig air supply pressure and checked for leaks. Three of the sensors were found leaking: No. 2 (ITSH-19112), No. 4 (ITSH-19117) and No. 5 (ITSH-19153). Sensor No. 2 was one of the jacket water temperature sensors installed on emergency diesel generator 1A during the incident. All three leaking sensors were methodically disassembled to determine the cause for the leaks. The relative positions of internal components were carefully marked to allow reassembly of the sensors to their as-received condition. Disassembly of sensor ITSH-19112 revealed pieces of pipe thread sealant and metal shavings on the viton seat of the poppet valve. The sensor was cleaned, reassembled, and recalibrated. The as-found trip setpoint was 162.2 °F. The licensee believes that the combination of foreign materials found inside the sensor and the low trip setpoint could explain the apparent intermittent behavior of the sensor during the incident. Disassembly of the other two leaking sensors also revealed metal shavings and pieces of thread sealant that appeared to affect operation of internal moving parts (i.e., the poppet spring and poppet valve). Sensor No. 5 had a 1/4-inch by 1/32-inch piece of thread sealant lodged on the viton seat. After the sensor was cleaned and calibrated, its trip setpoint was found to be 191.3 °F. Sensor No. 4 did not trip; bath temperature was increased to 210 °F.

Sensor No. 1 (ITSH-19111) was the other quarantined jacket water temperature sensor that was installed on emergency diesel generator 1A during the incident. This sensor was found to be venting during post-event testing. During subsequent troubleshooting, the air supply line at the sensor was crimped to allow pressure to build to 60 psig, and then released to pulse the sensor with air pressure. The sensor stopped venting after being pulsed several times. The sensor was not found leaking during testing at Wyle, and it was not disassembled. However, the vent cap was unscrewed, revealing both pieces of pipe-thread sealant and metal shavings. The vent cap is plastic and pipe sealant is not applied to its threads. The as-found trip setpoint was 188.7 °F.

Sensor No. 3 (ITSH-19146) acted sluggishly during testing (e.g., following reset, it took several minutes for supply pressure to return from 40 psig to within 1 psig of 60 psig). Disassembly and inspection of the sensor revealed pipe-thread sealant on the poppet spring and wedged between the side of the poppet well and the poppet valve. There were no foreign materials identified inside any of the sensors that originated from the air supply upstream of the sensor's air supply ports. In general, after the internals of the sensors were cleaned and the sensors were recalibrated, the quarantined sensors performed acceptably during subsequent testing.

The pieces of thread sealant found in the sensor internals were found to originate from the air supply port where the sealant (Neolube Pipe Thread Sealant No. 100) is applied to the Swage-Lock fitting before being screw-fitted into the sensor body. The sealant is designed to lubricate the threads and to provide a seal against pressure leakage caused by shock or vibration. The sealant is supposed to help prevent galling between the threads. The sealant can be used at high temperatures and remains somewhat pliable; it does not completely harden. It appears that the sealant was being used too liberally and being applied to close to the end threads of the fitting that first mate with the sensor. It is the licensee's practice to only use a fitting one time. A new sensor would receive a new fitting; the old fittings are not reused.

The metal shavings or splinters appeared to be originating from the air supply port screw threads of the sensor. It appears that the shavings (called thread spalls) are either dislodged from the screw threads or are created upon insertion of the Swage-Lock fitting. The Swage-Lock fitting is made of stainless steal, which is a harder material than the aluminum sensor body. Inserting the Swage-Lock fitting could be carving spalls from the sensor threads as it is being inserted.

Conclusion

Based on the results of the testing performed, the licensee believes the primary cause for the trips of emergency diesel generator 1A during the incident was improper intermittent operation of the Calcon jacket water temperature sensors. Intermittent operation appears to have been caused by the presence of foreign material (i.e., pipe thread sealant and thread spalls) that affected sensor internal moving parts. Premature venting of the sensor air supply lines can cause the engine control logic to sense a false high temperature trip condition and to automatically trip the emergency diesel generator. Contributing causes appear to include the effects of multiple leaks existing in the pneumatic engine control system, and sensor calibration techniques that may have resulted in lower setpoint values.

The licensee has experienced additional problems with Calcon pneumatic temperature sensors subsequent to the testing at Wyle. Specifically, emergency diesel generator 1B unexpectedly tripped on high jacket water temperature during testing. The Vogtle I&C shop had calibrated the sensors to trip at 200 ± 4 °F, but subsequent testing at Wyle found the setpoints to be between 160 °F and 165 °F. The licensee's preliminary investigation indicates that the relative locations of the reference temperature element and the sensor to the bath heater, and the circulating capability of the bath during sensor calibration, may have contributed to the lower setpoints. The licensee's troubleshooting efforts are continuing.

Subsequent to the Team's investigation, the lube oil pressure sensor (IPSL-4749A) that would not reset during post-incident calibration, and which may have been venting during the incident, was inspected and tested by the diesel generator supplier (Cooper Industries, formerly IMO Delaval Inc.). The sensor diaphragm was found to be pushed up against and sticking to the sensor's process pressure sensing port by the spring and pressure plate assembly on the sensor side of the diaphragm. This significantly reduced the cross-sectional area of the diaphragm exposed to process pressure, and a greater process pressure is required to unstick the diaphragm. The diaphragm did not break loose during testing until pressure was increased to 118 psi. Normal lube oil pressure when the engine is operating is approximately 55 psi. The sticking is a consequence of "tolerance stack-up" as discussed in an addendum dated May 12, 1988 to a 10 CFR Part 21 report from IMO Delaval Inc. to NRC.

The intent of the Part 21 addendum was to have the affected Calcon Model B4400 pressure sensors (that could not be verified to not have the problem) returned for remachining, inspection and testing. The problem fix was to further counter bore the sensor head to increase the area above the diaphragm on the process side to prevent the diaphragm from being able to make contact with the sensor head and process connection port. The corrected sensors were designated as Model B4400B. The sensors installed at Vogtle were believed not to have the problem and were not replaced.

The sensor set point is adjusted by changing the spring tension on the sensor side of the diaphragm. Spring pressure on the diaphragm over time may have caused the diaphragm to stretch, eventually creating the sticking problem, even if the sensor was verified to function properly during previous tests. In addition, inspection of the sensor revealed evidence of moisture in the sensor, specifically the pressure plate spring was rusted and sensor internal surfaces appeared to be stained, such as could be caused by dew formed by condensation. The diesel generator vendor speculated that the moisture problems may have occurred during plant construction when the engine was in storage. The sensors were installed on the engine by the vendor in August 1981. Some debris was also found in the sensor (a small metal sliver and several pieces of dirt). Therefore, possible causes that may have contributed to the sensor failure include debris in the sensor, aging and stretching of the elastomer diaphragm, and physically changing sensor properties during calibration (e.g., tolerance stack-up or diaphragm characteristics). The Transamerica Delaval Inc. Owners Group has recommended that the elastomers in the Calcon sensors be replaced every five years. The vendor is reevaluating the problem and the need to update the Part 21 report to address stretching of the diaphragm with age and whether to recommend that all Model B4400 sensors be replaced with the modified Model B4400B sensors.

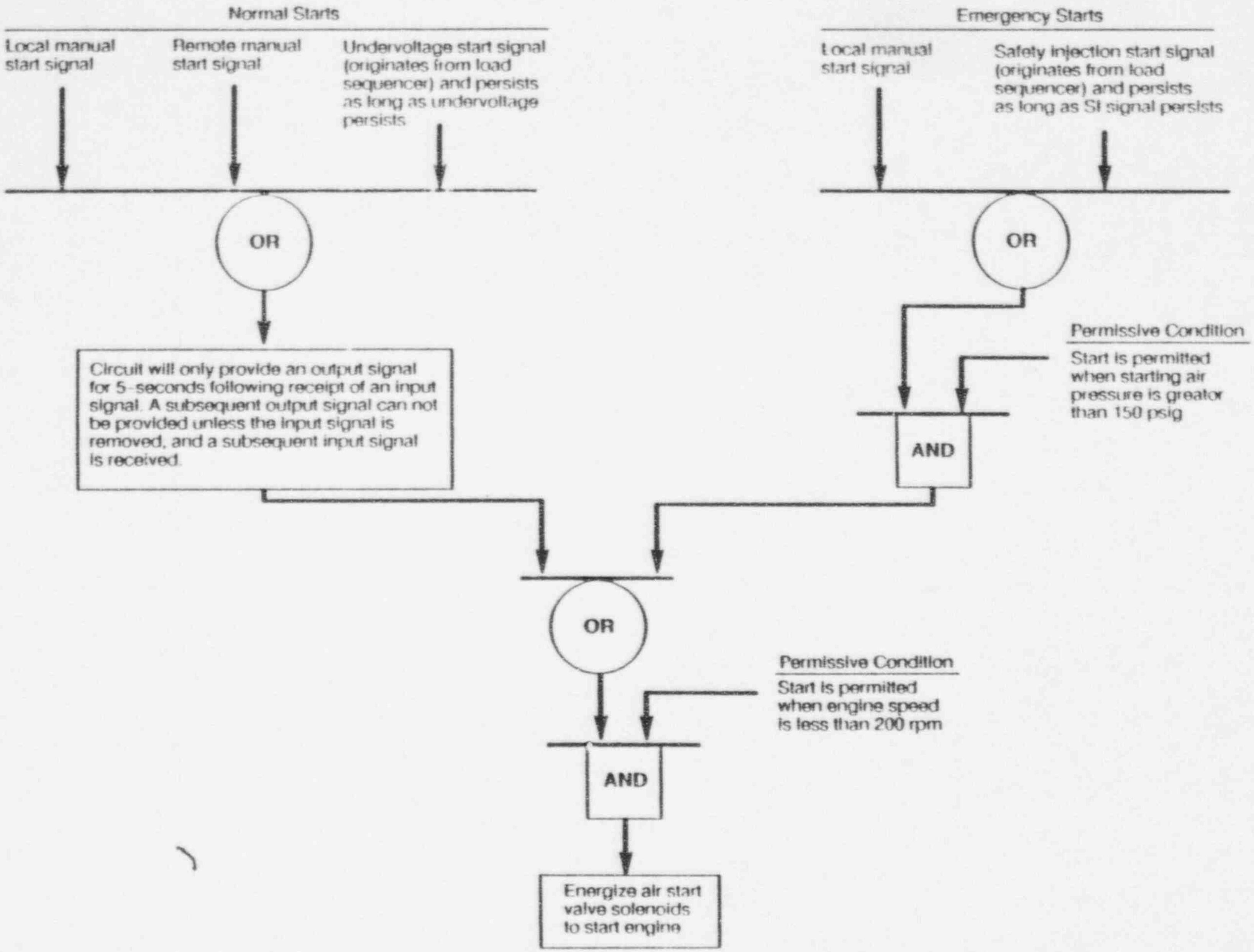
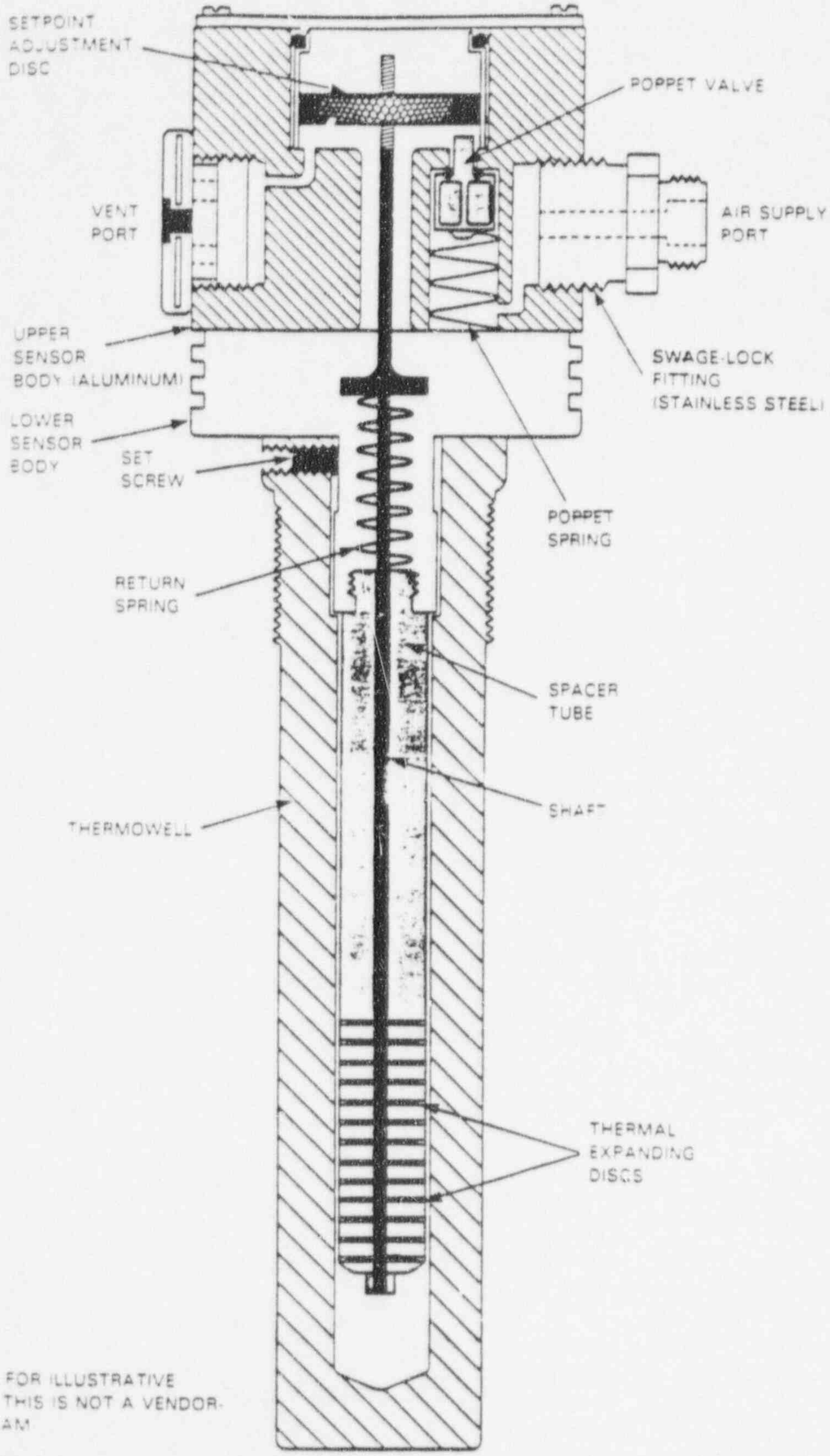


Figure J.1 Emergency Diesel Generator Start Logic (simplified Diagram)



THIS DIAGRAM IS FOR ILLUSTRATIVE PURPOSES ONLY. THIS IS NOT A VENDOR-APPROVED DIAGRAM.

Figure J.2 Calcon Pneumatic Temperature Sensor (Model A3500-W3)

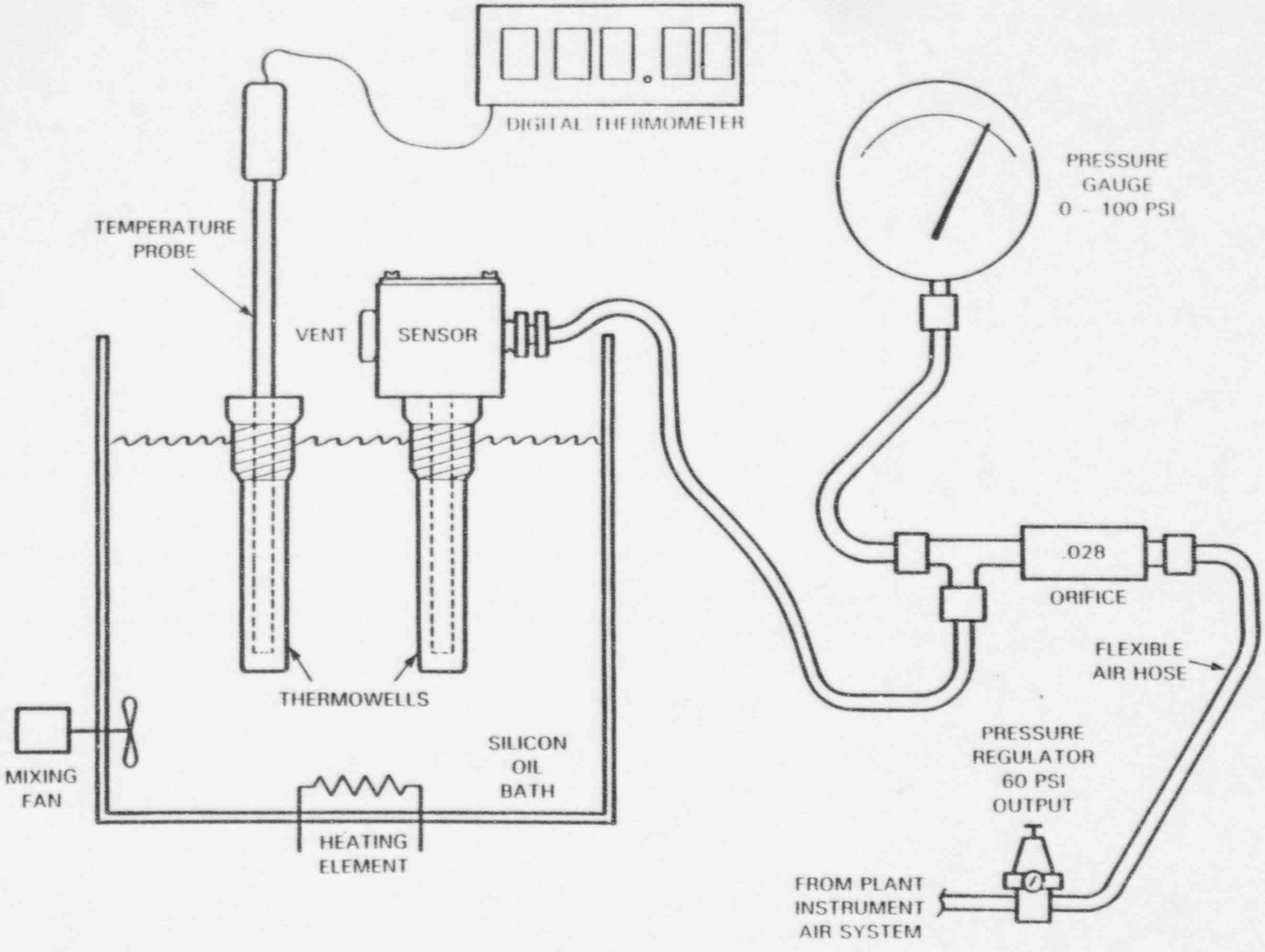


Figure J.3 Temperature Sensor Calibration Configuration

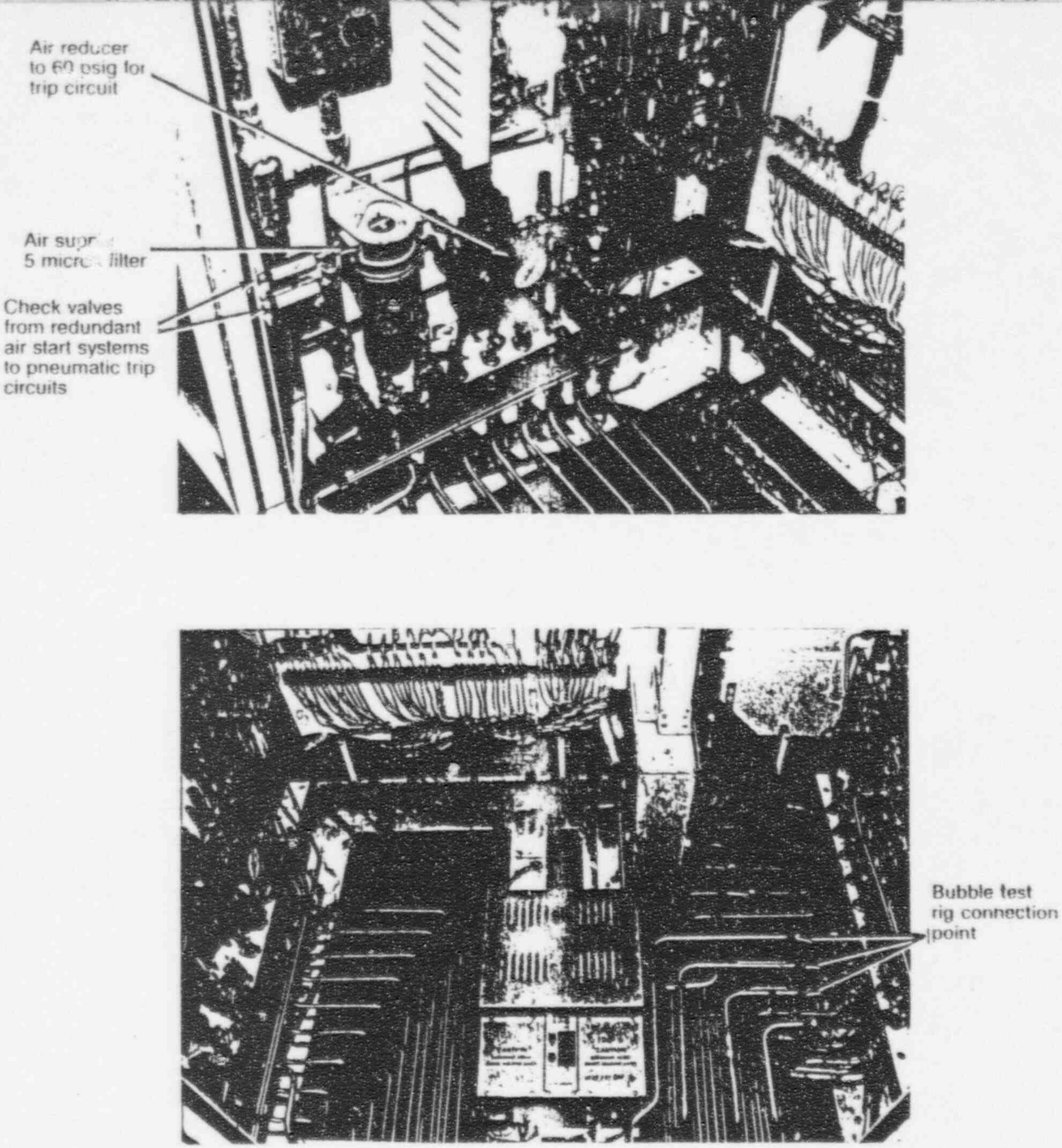


Figure J.4 Diesel Generator Trip Circuitry: Bottom Views

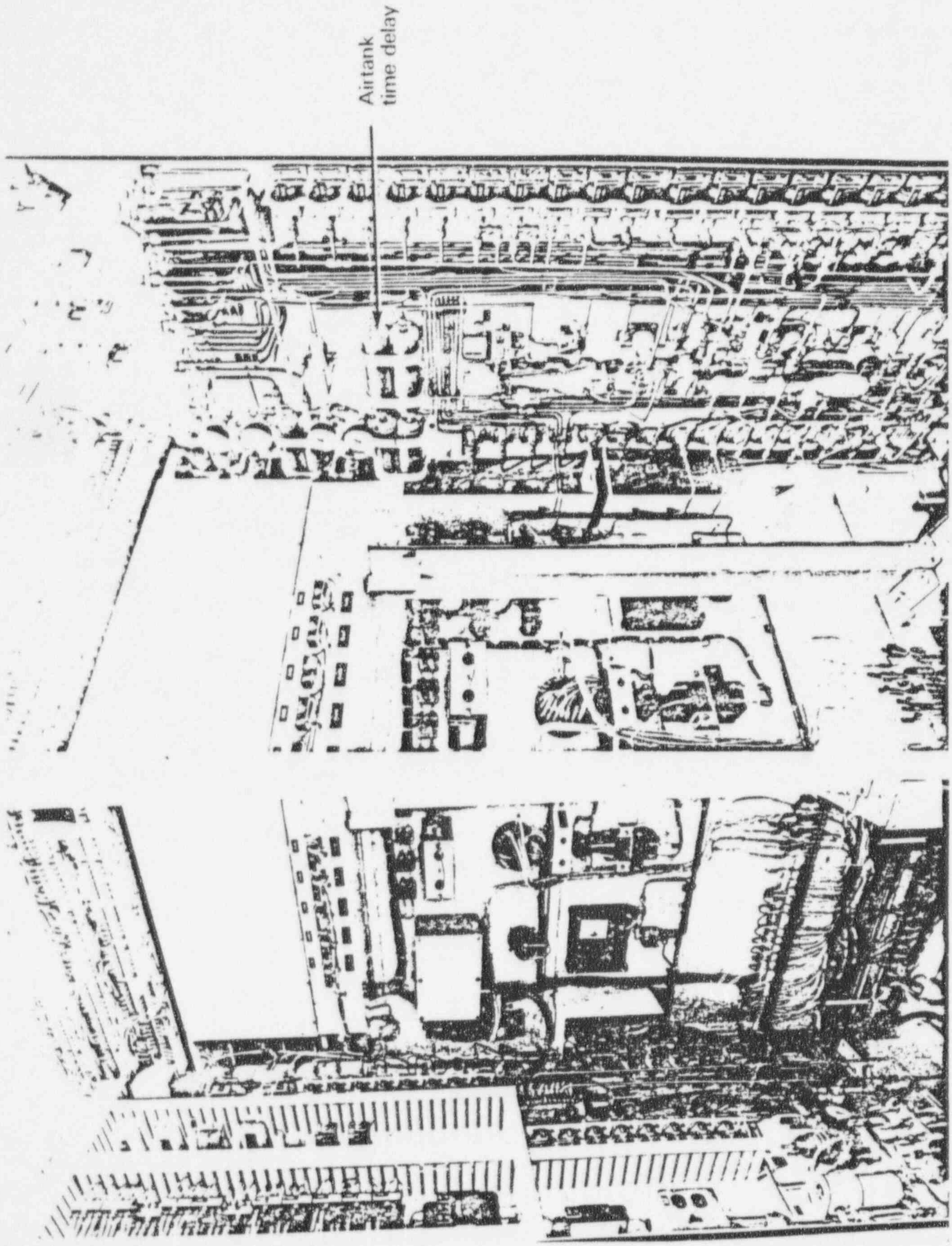


Figure J.5 Diesel Generator Trip C[illegible]ity: Left, and Right Views