UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, D. C. 20555

June 8, 1990

MEMORANDUM TO: J. Carroll, Chairman, Plant Operations Subcommittee

FROM: P. Boehnert, Senior Staff Engineer

SUBJECT: NRC INCIDENT INVESTIGATION TEAM (IIT) REPORT - LOSS OF VITAL AC POWER AND RHR DURING MID-LOOP OPERATIONS AT VOGTLE UNIT 1

We have just received an advanced copy of the subject IIT report, to be published as NUREG-1410. I have attached excerpts from the report that summarize: the "Problem Areas Leading Up to the Incident", a narrative account of the event, and the "Findings and Conclusions" of the IIT.

In summary, the IIT concluded:

- Adequate precursor information was available to make this incident preventable.
- The Vogtle staff generally handled the incident well.
- Significant potential generic lessons were identified, including:
  - Approaches to shutdown risk management need to be developed.
  - There is incomplete implementation of existing analysis and guidance into procedures and training.
  - There is a need for additional analysis of reactor coolant system behavior following the loss of the residual heat removal system.
  - There is a need for further synthesis of existing operating information.
  - Emergency classification guidance and implementation problems exist.
  - The technical specifications do not take into consideration of risk associated with the various

configurations of systems that may exist during shutdown conditions.

- At least some diesel generator control and annunciator systems are complex and may not be well understood.

The Commission is scheduled to be briefed by the Team this morning. I plan to attend this briefing and will report the results to you. A briefing by the IIT to the ACRS is scheduled during the August meeting.

Attachment

cc: ACRS Members
ACRS Technical Staff
S. Long, ACRS Fellow

Finally, Section 10 presents the Team's findings and conclusions relative to this incident.

The appendices provide a considerable amount of background information for the material presented in Sections 1 through 10. This information is provided for those readers who desire more details in a particular area.

The Team has concluded this investigation and provided its findings and conclusions to the Nuclear Regulatory Commission and the industry for their consideration and for the possible development of follow-on actions.

1.2 Problem Areas Leading Up to the Vogtle Incident

A combination of nonconservative initial conditions, combined with the failure to adequately control switchyard work activities, led to the Vogtle incident. Shutdown electrical redundancy was limited to only two of four safety bus power supplies. Following the loss of the one in-service reserve auxiliary transformer, the one "operable" emergency diesel generator malfunctioned.

- Switchyard Controls

The Vogtle staff had no effective control over a fuel and lubricants truck conducting routine operations in the switchyard. Moreover, because the truck carried fuel, there was the risk of a conflagration from ignition of fuel caused by electrical arcing. The damage to the switchyard equipment from such an event would have further limited the Vogtle staff's ability to recover electrical power. Guidance identifying the need for additional controls and precautions for work on electrical equipment, including work in the switchyard, had been provided to the industry.

- Redundancy of Shutdown Electrical Supplies

The Vogtle staff has tentatively concluded that maintenance on two of the four safety bus power supplies could have been scheduled outside the period of mid-loop operations.

- Diesel Generator Reliability

The preliminary evaluation of the diesel generator trips indicates that the most probable cause of the trips involved the failure of Calcon jacket water temperature trip sensors. The investigation of the root cause of the failures was incomplete as of the date of issuance of this report. A significant number of Calcon sensor failures has occurred at Vogtle since 1985.

1.3 The Vogtle Staff's Handling of the Incident

The Vogtle staff generally handled the incident well, showing an effective response that compensated for weaknesses in their procedures. The Team identified some weaknesses,

however, in their ability to cope with the condition that would exist had the residual heat removal system not been returned to service.

The equipment hatch was shut in a timely fashion during this incident, and closure was initiated before their procedure directed them to do so. However, their demonstrated capability did not indicate that they could close the hatch in the 57 minutes that their analysis showed was necessary in the bounding case. Instead, they closed the hatch in 79 minutes and under more favorable conditions than assumed in their analysis. For example, if a similar incident occurred with a loss of all ac power, it would likely take several hours to shut the hatch using manual rigging.

The Vogtle staff was also effective in closing the reactor coolant system, considering that no procedures had been developed for this contingency. In fact, it appears that no industry-wide guidance has been developed on this issue.

Various recommendations from NRC Generic Letter 88-17 had been implemented. Specifically, the Vogtle staff had essentially redundant water level indication and reactor coolant system temperature indication from two operable core-exit thermocouples. The operations staff was aware of some of the alternate core cooling methods that were available.

Command, Controls, and Communication of Emergency Activities

The Vogtle staff experienced several communications problems during the incident. The pressurizer manway was installed because of a communication error, in spite of the shift superintendent's direction that it not be installed. Its installation had no significant impact on the incident because of the timely recovery of the residual heat removal cooling system and the fact that steam generators were available to provide reflux cooling.

The operators indicated that they planned to use gravity-fed water to remove decay heat while preventing boiling if the residual heat removal system had been lost for a longer period. In this case, the lack of a reactor coolant system vent path, typically the pressurizer manway, would cause the reactor coolant system pressure to rise, eventually disabling gravity fill capability and leading to boiling after several hours. Maintaining a gravity fill capability with an open vent could extend the time to boiling.

There was some difficulty controlling emergency activities. Accounting for personnel in the protected area was a problem because a large number of personnel were on site, and many were involved in activities to mitigate the loss of power and loss of the residual heat removal system. The staff used this outage manpower to initiate reactor coolant system closure, containment building closure, and restoration of safety ac power before the emergency plan was activated. However, in the subsequent turnover to the emergency response organization, the personnel involved were unaware of the pressurizer manway status due in part to personnel changing roles and previous communication errors. Procedures did not exist to provide guidance on how to use existing bus connections and other potentially available sources to restore power to safety buses in an emergency.

The Vogtle staff experienced a delay in shutting the steam generator manways because the workers involved were pulled off the job to leave the containment building because of a communication error.

Communications problems also existed in notifying offsite authorities of the declaration of a Site Area Emergency. This occurred because Vogtle personnel did not fully understand their primary and backup emergency notification systems. As a result, notifications were made late, especially for the State of Georgia and Burke County.

Incident Classification Issues

The Vogtle staff appropriately classified the incident as a Site Area Emergency in spite of ambiguous classification procedures. A survey of classification procedures from 12 other sites confirmed that a loss of power event similar to Vogtle's could have been initially classified from "no emergency at all" to a Site Area Emergency. The guidance in NUREG-0654 for classification of loss of power events is unclear. ("Criteria for Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of Nuclear Power Plants," Revision 1, November 1980.) NUREG-0654 is generally focused on events initiating from power operation. It does not provide specific guidance for classifying the scope of events that can occur during cold shutdown. These events may have a greater urgency because of a lack of containment building integrity, lack of reactor coolant system integrity, and degraded heat removal capability.

Diesel Generator Trips

The load sequencer and diesel generator control systems are complex and their operation during the incident was not fully understood by the Vogtle staff, although the systems functioned as designed. In addition, the Vogtle staff had difficulty determining the cause of diesel generator trips during the incident because of incorrect annunciator panel reset practices and because of shortcomings in the human factor design of the trip alarm identification system.

Shutdown Operation Risk Management

In evaluating practices for outage scheduling, it was found that the Vogtle staff depends almost exclusively on technical specifications to ensure an adequate level of safety. For example, having only two sources of ac power in service is allowed during cold shutdown by technical specifications, but may not be prudent during mid-loop operation. Vogtle made no attempt in their outage planning to shift this configuration to a less sensitive time during the outage. Precursor information also indicates that there may be a higher probability of loss of remaining safety power as a result of outage activities.

In general at Vogtle and other PWRs, there is no technical specification requirement that the equipment hatch be shut in mid-loop operation, as is required for refueling operations,

even though the core damage that could occur from a mid-loop incident is greater than would be expected from a fuel-handling accident. This is a particular concern when high decay heat rates exist.

Technical specifications for cold shutdown and refueling operations were not developed based on a comprehensive safety analysis, including determining whether or not single-failure criteria should apply, as are the technical specifications for power operation. The lack of a comprehensive basis provides an opportunity for plant staffs to overlook conditions, such as events that could lead to uncovering the core.

Coping with Extended Loss of the Residual Heat Removal System

Progress has been made in implementing improvements in this area since the Diablo Canyon incident in 1987 in response to Generic Letter 88-17 recommendations. However at Vogtle, the equipment hatch closure process had not been proceduralized to incorporate the results of their recent analysis. There is a need to consider further analysis regarding, for example, the possibility that reflux cooling may start and stop as a result of thermohydraulic effects and the potential for misleading instrument indications. What is learned from analysis in this area will have an impact on the alternate core cooling strategy guidance to be provided to operators.

Feedback to the Industry

An extensive amount of documentation was identified by the Team, including 74 loss-of-ac events during shutdown, and 52 loss-of-residual-heat-removal events during mid-loop operations. Also, 44 operating experience documents were provided to the industry regarding the above events. The Vogtle staff emphasized their need for specific guidance in industry feedback documents and gave the impression that they were limited in their ability to extrapolate beyond the actual events discussed in the guidance. There appears to be a need to develop a set of broader recommendations from the vast amount of specific operating event information available. Generic Letter 88-17 attempted to do this for the loss of residual heat removal issue and was partially successful. However, it did not address specifics in all appropriate areas, such as redundancy of electrical power sources.

1.4 Summary

In summary the Team concluded:

- Adequate precursor information was available to make this incident preventable.
- The Vogtle staff generally handled the incident well.
- Significant potential generic lessons were identified, including:
  - Approaches to shutdown risk management need to be developed.

- There is incomplete implementation of existing analysis and guidance into procedures and training.
- There is a need for additional analysis of reactor coolant system behavior following the loss of the residual heat removal system.
- There is a need for further synthesis of existing operating information.
- Emergency classification guidance and implementation problems exist.
- The technical specifications do not take into consideration the risk associated with the various configurations of systems that may exist during shutdown conditions.
- At least some diesel generator control and annunciator systems are complex and may not be well understood.

2 NARRATIVE OF THE INCIDENT

This section provides a narrative description and a tabular sequence of events for the loss of decay heat removal capability and loss of safety-related ac power at Unit 1 of the Vogtle Electric Generating Plant (Vogtle) on March 20, 1990. The NRC Incident Investigation Team (the Team) created this narrative and the chronological sequence of events listed in Table 2.1 from data available from the plant emergency response facility computer, operator and management interviews, logs kept by site personnel, and interpretations of data and trend recordings.

The emergency response facility computer, which ordinarily records data automatically, had to be initiated manually after the incident began to save relevant historical data. In addition, the emergency response facility printer in the control room did not record alarm data because it lost power when the incident started. A manual reset from the programmer's console was required but not performed. Some event data was also missing because of an emergency response facility computer hardware problem during the incident (see Sec. 3.7 for a discussion of this issue). For most of the incident, however, data from the emergency response facility computer were adequate to reconstruct the sequence of events.

The data collection systems at Vogtle do not record data to facilitate the diagnosis of diesel generator trips. In addition, the operators did not identify and record the alarms that occurred when the diesel generator first tripped. Thus, reconstruction of the sequence of alarms associated with this trip was not possible.

The licensee's corporate policy is to refer to the time that events occur using Central Standard Time (CST), which is the time zone for the corporate office in Birmingham, Alabama, instead of Eastern Standard Time (EST), which is the time zone for Vogtle. Although the Team reviewed many licensee records during this investigation that used both EST and CST (Fig. 2.1), EST is used throughout this report because the plant is located in that geographical region.

2.1 Plant Status Before the Incident

The reactor had been shut down on February 23, 1990, for a scheduled 45-day refueling outage. It was the second refueling outage for this unit and for the site. By March 20, fuel had been reloaded into the reactor core, the first of two passes to tension (i.e., tighten) the reactor vessel head studs was complete, and the outage team was waiting for permission from the control room to begin the final tensioning. Water in the reactor coolant system was being maintained at approximately 187 feet 9 inches, which is 5-1/2 inches below the top of the hot leg pipe and 9 inches above the centerline of the pipe. The 1A residual heat removal pump was in service to provide decay heat removal. The reactor coolant system temperature was being maintained at approximately 90 °F according to readings from the two connected core-exit thermocouples. The required borated emergency water source was being maintained in the refueling water storage tank at 78.8 percent of capacity (approximately 580,000 gallons), with a boron concentration of 2457 parts per million (ppm).

The steam generators were in wet layup and the ECCS accumulators were not in service. The emergency boration flow path was from the refueling water storage tank through the 1A centrifugal charging pump, which was aligned with the alternate charging flow path because of maintenance work on the normal flow path. A gravity-feed makeup operation to maintain the reactor cooling system water level, using the emergency boration flow path, was in progress at the time of the incident. The circuit breakers for the 1A and 1B safety injection pump motors were in a racked-out position (so that they were inoperable) as required by the plant's technical specifications. The breakers could be racked in within approximately 5 to 10 minutes if the pumps were needed for reactor system makeup and cooling should residual heat removal capability be lost. Unit 2 was operating at 100 percent power in a normal electrical alignment.

2.2 Inoperable Equipment and Abnormal System Alignments

As is normal during a refueling outage, maintenance was in progress on a variety of systems and equipment so that some equipment was out of service and several systems were in abnormal configurations.

For example, the 1B emergency diesel generator was out of service for scheduled 36-month maintenance and surveillance inspections. The 1B reserve auxiliary transformer had been removed from service for an oil change. The 1B safety bus was being powered from the 1A reserve auxiliary transformer through its alternate supply circuit breaker. The nonsafety buses for Unit 1 were energized from the 230-kV switchyard through the main transformer and the unit auxiliary transformers (Fig. 3.2).

The 1B centrifugal charging pump flow path was out of service for valve maintenance, leaving the 1A centrifugal charging pump and the positive-displacement charging pump available to inject water if needed. The chemical and volume control system letdown flow path had been out of service for a variety of maintenance activities and was being aligned before being returned to service. When controlling water level at mid-loop, Vogtle administrative procedures require that the letdown flow path be "tagged out" (i.e., marked as being out of service), to reduce the likelihood of inadvertent draining of the reactor coolant system.

The reactor coolant system water level was being maintained at mid-loop for the following work:[1]

- The No. 4 accumulator isolation valve had been disassembled for repairs. This left reactor coolant system integrity only partially compromised because there are two check valves between the No. 4 accumulator isolation valve and the reactor coolant system.

---

[1] Mid-loop refers to conditions that exist when the reactor coolant system water level is lower than the top of the flow area at the juncture of the hot legs with the reactor vessel (see Figures 3.19 and 3.22).

- The normal charging check valve for the chemical and volume control system was also disassembled for repairs, leaving the alternate path available for charging.

- All steam generator nozzle dams had been removed, but only steam generators 1 and 4 had their primary manways completely installed. Maintenance personnel were restoring the primary manways on steam generators 2 and 3. In addition, the pressurizer manway was removed to provide a vent path for the reactor coolant system.

The containment building equipment hatch was open to allow workers to remove equipment, and the containment building personnel hatch was open to facilitate worker access. Some equipment was blocking the containment building equipment hatch; however, no hoses or air lines were running through the hatch because special containment building penetrations had been constructed in anticipation of the need to quickly close the containment building during an outage.

In summary, just before the incident, the reactor coolant system was open for maintenance, the reactor vessel water level was lowered, fuel had been loaded in the vessel, the containment building was open, and two of four safety-bus electrical power sources were out of service.

2.3 Incident Initiator

On March 20, 1990, at approximately 9:17 a.m., a truck driver accompanied by a security escort entered the protected area with the site's fuel and lubricants truck. The driver was scheduled to refuel air compressors and welding machines located around the site during the Unit 1 outage. Plant procedures required that this vehicle not be allowed in the protected area without a security escort.

The driver had performed these duties on an irregular basis for about a year. In the past, he had to back into the switchyard so that the truck's fuel hoses would reach the equipment being refueled. On this morning, he drove straight in because the temporary equipment that required him to back into the switchyard in the past had been removed. After checking, he found that the welding machine did not need to be fueled. He then got back into the truck and was backing up when the truck hit a support pole for the C phase of the 230-kV feeder line supplying offsite power to the 1A and 2B reserve auxiliary transformers. The insulator fractured, the line fell to the ground, and the transformer breakers tripped because of a phase-to-ground fault (see Figs. 2.3 and 2.4 for location).

2.4 Loss of Electrical Power and Recovery

Before the incident, one reserve auxiliary transformer (1A) was supplying power to Unit 1's safety-related equipment, and one emergency diesel generator (1A) was in standby. At 9:20 a.m., the 1A and 2B reserve auxiliary transformer high side and low side circuit breakers tripped because of the phase-to-ground fault caused by the fuel and lubricants truck. The trip caused a loss of offsite power to the 1A and 1B 4160-V safety buses and the Unit 2

B safety bus. Loss of power to the 2B reserve auxiliary transformer should not have resulted in a Unit 2 trip. However, a wiring error had been made during plant construction on the main generator differential protection current transformers that caused the Unit 2 trip. The plant staff was aware that the current transformer tap setting had not been functionally tested and had planned to do the test in the future. The 1A and 2B emergency diesel generators started and loaded successfully.[2]

Upon the initial loss of offsite power, the 1A emergency diesel generator started automatically because of the undervoltage on its respective safety bus, carried loads for 80 seconds, then it tripped (stopped). Following the trip, it locked out, as it was designed to do, to prevent a subsequent automatic start on undervoltage. However, the trip and lockout were unexpected by the operators. The conditions that tripped the emergency diesel generator at this time, while not known for certain, are believed to have been caused by sensor problems similar to those that caused the second trip (see Sec. 3.2 for a detailed discussion of the trip and lockout).

The operators did not record the diesel generator trip conditions that were annunciated before resetting and clearing the annunciator panels. Trip conditions annunciated for diesel engines are not automatically recorded. Since the annunciator response control switches are shared for the diesel generator and safety bus annunciator panels in the control room, it is possible that the operators reset and lost the trip alarms for the diesel generator in the process of responding to safety bus alarms (see Fig. 2.2 for control room layout). Equipment operators arrived at the diesel generator room several minutes after the first trip, but cleared the alarms at the local engine control panel before trip conditions were recorded. By this time, a maintenance foreman and a mechanic had also entered the emergency diesel generator room.

Approximately 18 minutes after the 1A emergency diesel generator tripped, it was restarted. Following the second start, it carried the load for 70 seconds and tripped off again. Trip signals were observed for high jacket water temperature, low jacket water pressure, and low turbocharger oil pressure. Any one trip signal alone would have been sufficient to cause a diesel generator trip. All of these trip signals are generated by pneumatic (air-operated) sensors.

The high jacket water temperature conditions require the activation (or incorrect operation) of two of three sensors to cause a trip. The operators reported that the three trip signals appeared to come in simultaneously. One operator reported after the trip that he had observed normal jacket water temperature. During the incident the operators believed that the second trip was caused by low jacket water pressure. This belief provided a basis for the hope that an emergency mode start would be successful because it blocks this type of trip. Later, however, low jacket water pressure was discounted as a cause of the trip signal because the maintenance foreman observed normal jacket water pressure. Later analysis

[2] This report focuses on the event at Unit 1; Unit 2 will not be referred to except when necessary.

revealed that the high jacket water temperature trip was the most probable cause of the second diesel generator trip. The root cause determination was not completed at the time this report was published.

At 9:56 a.m., after 15 minutes of unsuccessfully attempting to find the cause of the trips and 36 minutes into the incident, the emergency diesel generator was again started, using manual emergency start rather than a normal undervoltage start. The intent of the emergency start was to have all but the four most crucial trips blocked. The emergency start bypassed the low jacket water pressure trip, which the operators believed caused the second shutdown. The generator did start, load, and continue to run without further incident, restoring ac power to one safety bus. No annunciations of trip conditions, whether blocked or unblocked, were received either in the Unit 1 control room or the diesel generator room. However, two non-trip warning alarms were received that operators estimated lasted about one minute each. They were for:

- High lube oil temperature - subsequent testing showed that this alarm occurs spuriously upon receipt of the low lube oil sensor malfunction alarm listed below
- Low lube oil pressure sensor malfunction - this malfunction indicated that one of three low lube oil pressure trip sensors had actuated (two of three are needed for a trip)

The 1A emergency diesel generator was run for 3 hours and 1 minute, until 12:57 p.m., as the sole power source to the 1A safety bus. At 11:40 a.m., 2 hours and 20 minutes into the incident, the 1B reserve auxiliary transformer was energized to supply power to the 1B safety bus. At 12:57 p.m., the 1B reserve auxiliary transformer was connected in parallel to the 1A safety bus. The resulting lineup provided two sources (the 1A emergency diesel generator and the 1B reserve auxiliary transformer) to the 1A safety bus. The 1A emergency diesel generator was run in parallel with the 1B reserve auxiliary transformer from 12:57 p.m. until the 1A emergency diesel generator was shut down at 2:26 p.m. The 1A emergency diesel generator was returned to a standby configuration at 3:05 p.m.

2.5 Restoration of the Reactor Coolant System Boundary

At the initiation of the incident, the reactor coolant system pressure boundary was breached by the following circumstances:

- The reactor vessel thermocouple lead penetration seals (conoseals) were open.
- Manways for steam generators 2 and 3 were in place, but not fully installed.
- The chemical volume and control system normal charging check valve was disassembled.

- The No. 4 accumulator isolation valve bonnet stud nuts were not installed.

- The pressurizer manway was open as a vent path for the reactor coolant system.

At approximately 9:35 a.m., about 15 minutes into the incident, the shift superintendent directed the outage and planning manager to close the reactor coolant system, with the exception of the pressurizer manway, which was to be left open to provide a reactor coolant system vent path. The outage and planning manager instructed the maintenance supervisor to complete the following tasks before maintenance personnel left the containment building and for which maintenance work orders already existed:

- Complete the reassembly of emergency core cooling system accumulator No. 4 isolation valve.

- Reassemble the fully disassembled normal charging line check valve.

- Complete installation of the manways for steam generators 2 and 3.

- Verify that the pressurizer manway was removed.

- Close the equipment hatch and reinstall the personnel access hatch interlocks for the containment building.

The manager of health physics and chemistry had previously been directed by the shift superintendent to ensure that all personnel leave the containment building in an orderly manner, although his instructions for evacuating personnel working on the reactor coolant system closure were unclear. As a result, the maintenance personnel who were working on the steam generator manways before and during the incident were instructed by health physics personnel to leave the containment building. Thus, they began to remove their protective clothing in preparation for leaving the containment building.

In the meantime, the shift superintendent realized that his instructions to evacuate the containment building conflicted with his direction that workers remain to seal the reactor coolant system. The shift superintendent called the manager of health physics and chemistry back to clarify who should leave the containment building and who should stay to continue work. The maintenance personnel who were removing their protective clothing were then told by a maintenance supervisor to return to the containment building to finish installing the remaining steam generator manways. After donning protective clothing and respirators, the maintenance personnel (assisted by health physics personnel) returned to the steam generator area. At about this time, they heard the announcement that a Site Area Emergency had been declared. It was 10:01 a.m., 41 minutes into the incident. Upon hearing this announcement, the maintenance personnel decided to tighten all bolts for the manways, using a long-handled wrench and sledge hammer to complete the work as expeditiously as possible and still ensure that the bolts were tight. Closure of the steam generators was completed and the control room was notified of the closure over the public address system

at approximately 10:34 a.m., 1 hour and 14 minutes into the incident, after attempts to contact the control room using the plant phone system had failed.

A communications misunderstanding led the manager of health physics and chemistry to believe that all reactor coolant system openings, including the pressurizer manway, should be sealed. Consequently, when the supervisor of the steam generator work was leaving the containment building, he was informed that the pressurizer manway would have to be closed. Using some of the workers who had just finished closing the containment building equipment hatch at 10:42 a.m., he completed installation of the pressurizer manway at 11:40 a.m., 2 hours and 20 minutes into the incident.

The licensee had reached the desired reactor coolant system configuration, except for the fact that the pressurizer manway was shut and the reactor vessel head thermocouple seals (conoseals) were not installed. The reactor coolant system boundary was sealed other than for the conoseals. Electrical power had been restored and the residual heat removal cooling system had been re-established when control room operators were informed that the pressurizer manway had been closed. The general manager, who had by now assumed the emergency director's position, ordered the manway reopened at 12:04 p.m., but ordered it left shut at 12:21 p.m. because the plant was in a stable condition.

2.6 Restoration of Decay Heat Removal and Makeup Capabilities

The 1A residual heat removal system loop was cooling the reactor core before the loss of power. The 1B residual heat removal pump was available through the loop cross-tie, although the 1B loop injection valve was closed for maintenance. A gravity flow from the refueling water storage tank to the reactor coolant system was in progress before the incident and was available by local manual activation throughout the incident. The Unit 1 shift supervisor ordered the gravity flow path to the vessel from the refueling water storage tank isolated by locally closing the motor-operated isolation valve, which had been open when ac power was lost. He ordered this path isolated because the desired amount of makeup water had been added.

When power was lost at 9:20 a.m., the 1A residual heat removal pump tripped and was not restarted until power was restored to its bus at 10 a.m., 40 minutes into the incident.

At the time of the incident, three sources of vessel water level indication were available (two gages in the control room and one inside the containment building). Two thermocouples were connected to the ERF computer and displayed in the control room. When the 1A residual heat removal pump was started at 10 a.m., the thermocouple temperature had risen to 136 °F. The reactor coolant system was subsequently cooled down and maintained at less than 110 °F.

At 12:31 p.m., 3 hours and 11 minutes into the incident, the 1B residual heat removal pump was started. The 1A residual heat removal pump was placed in a recirculation mode to minimize the risk of losing residual heat removal capability while connecting the

1A diesel generator in parallel with offsite power on the 1A safety bus. At 3:16 p.m., 5 hours and 56 minutes into the incident and after the 1A diesel generator was placed in standby, the 1A residual heat removal pump was placed in service and the 1B residual heat removal pump was placed in recirculation and then stopped.

The following sources of borated makeup water were available during the incident:

- Gravity flow from the refueling water storage tank (using local manual control) to the reactor vessel.

- Two safety injection pumps with breakers racked out and available in 5 to 10 minutes if power was available to the required safety bus.

- One centrifugal charging pump if power was available to the required safety bus.

- The positive displacement charging pump powered from nonsafety power. Cooling for this pump is powered from safety power. The plant staff stated that temporary cooling could be rigged from other available sources, although this had not been substantiated by testing. Thus, the availability of this pump is unclear.

The steam generators were available as a potential heat sink.

2.7 Establishment of the Containment Building Barrier

At approximately 9:35 a.m., 15 minutes into the incident, the Unit 1 shift superintendent directed that the containment building be closed. Before the incident, the containment building equipment hatch had been removed and was resting on mechanical stops. Portions of the two hatch cover hoist mechanisms were removed from the containment building for maintenance and, thus, were inoperable. However, because the hatch cover had been raised to the open position using the containment building polar crane, the hatch was still rigged to be moved using this crane. The polar crane is powered from nonsafety ac power, which was available throughout the incident. A significant amount of equipment was in the open hatchway at the outset of the incident, and a steel plate covered the area normally occupied by the hatch cover when it is in the closed position. A portable railway track used for moving a cart carrying equipment into and out of the building rested on the steel plate. In addition, a substantial amount of disassembled scaffolding was laying on the railroad tracks. A self-propelled crane, which was available nearby, was used to remove the steel plate from the hatch area. At approximately 10:42 a.m., 1 hour and 22 minutes into the incident, maintenance personnel lowered the containment building hatch and secured it in place using 8 bolts. They reported to the control room that the containment hatch was closed and then installed the remaining bolts. At about 11:03 a.m., 1 hour and 43 minutes into incident, the personnel airlock interlock was made functional, thus establishing the containment building as a barrier to the release of radioactivity. The maintenance personnel who had completed the closure of the reactor coolant system and containment building left the building by 11:50 a.m., 2 hours and 30 minutes into the incident. The availability of nonsafety power

for the polar crane improved the speed for installation of the containment building equipment hatch (see Sec. 3.6 for additional details).

2.8 Emergency Plan

A Site Area Emergency was declared at 9:40 a.m., 20 minutes into the incident, because Vogtle management interpreted the loss of all offsite and onsite ac power to the *safety* buses for more than 15 minutes to be equivalent to the emergency action level in the Vogtle procedure which indicates that loss of *all* offsite and onsite power for greater than 15 minutes is a Site Area Emergency. The emergency director signed the notification form used to inform offsite governmental agencies of the emergency at 9:48 a.m., 28 minutes into the incident. The Emergency Notification Network communicator then attempted to notify offsite agencies, using the control room primary Emergency Notification Network to State officials in Georgia and South Carolina. The control room primary Emergency Notification Network was inoperable because of the loss of safety power. The primary Emergency Notification Network receives power from the B train safety bus, which was deenergized until 11:40 a.m.

The Emergency Notification Network communicator shifted to the South Carolina backup Emergency Notification Network and established communications with the South Carolina Emergency Preparedness Division, and the Department of Energy's Savannah River Site at Aiken, Allendale, and Barnwell Counties at approximately 9:57 a.m., 37 minutes into the incident and 17 minutes after the Site Area Emergency was declared. Transfer of information to these agencies was completed at approximately 10:13 a.m., 53 minutes into the incident.

The Georgia Emergency Management Agency (GEMA) was contacted using the Unit 2 commercial telephone, which is the designated backup means of communication to GEMA and the Burke County Emergency Management Agency, at approximately 10:15 a.m., 55 minutes into the incident. However, no notification message was transmitted during this contact because of communicator confusion. When the control room Emergency Notification Network communicator contacted GEMA on the commercial telephone, the technical support center Emergency Notification Network communicator was confirming the operability of the primary Emergency Notification Network to Georgia and South Carolina as part of its role in activating the technical support center. The Emergency Notification Network in the technical support center was operable because it received power from the security diesel generator, which was operating properly. The commercial telephone contact between the control room and GEMA was terminated because both parties assumed that the notification would be transmitted via the Emergency Notification Network. In fact, the technical support center Emergency Notification Network communicator did not have the notification form and could not pass on the required information. Attempts by GEMA to obtain the notification information were successful at 10:35 a.m., 1 hour and 15 minutes into the incident, when the South Carolina Emergency Preparedness Division sent GEMA the completed notification form by facsimile. Vogtle established communications with GEMA at 10:40 a.m. and passed the notification information successfully by commercial telephone. Subsequent notifications

were made without difficulty. The primary Emergency Notification Network in the technical support center was used to transmit messages after the fourth message was sent to offsite agencies.

The initial notification to the Nuclear Regulatory Commission was made at 9:58 a.m., 38 minutes into the incident, from the control room on a commercial telephone because the communicator believed that the dedicated Emergency Notification System phone was out of service. Subsequent updates from the control room and technical support center were completed without major problems, except for a telephone problem, which resulted in the connection between Vogtle and the Nuclear Regulatory Commission repeatedly being interrupted. Each time the connection was interrupted, the Nuclear Regulatory Commission Headquarter's Operations Officer had to re-establish communications. The Nuclear Regulatory Commission Headquarters Operations Center and Region II Incident Response Centers were quickly staffed, but the NRC did not enter the Standby mode until about 1 hour later because it appeared that the 1A emergency diesel generator was operating normally and that the 1B reserve auxiliary transformer would be returned to service shortly.

The primary means for notifying onsite personnel in the protected area is the plant public address system (plant page). The primary means for notifying personnel outside the protected area, but inside the owner-controlled area, is the normal phone system. In general, these notifications were made; however, in some areas of the plant, the messages were not heard and those that were heard created some confusion because of the use of nonstandard terminology.

The plant page announcement of the Site Area Emergency was made at 10:01 a.m., 41 minutes into the incident. It was heard in all areas of the protected area except for some areas inside the containment building, on the turbine deck of the turbine building, and in the diesel generator building. Personnel in these areas were notified informally by word of mouth by their supervisors or by observing others leaving an area within approximately 10 minutes of the page announcement. Personnel in the buildings outside the protected area were notified by telephone calls from security personnel by 10:17 a.m., 57 minutes into the incident.

The announcement stated (1) that a Site Area Emergency had been declared, (2) that all visitors and their escorts should report to the Plant Entry Security Building, and (3) that all emergency response personnel should report to their assigned emergency response facility. The prescribed section of the initial announcement that would have instructed nonessential personnel to leave the protected area and proceed to the assembly area or to leave the protected area and proceed home was purposely omitted. Therefore, neither a total site evacuation nor an assembly and accountability procedure was initiated. The emergency director decided to omit this section because there was no immediate radiological danger to plant personnel and personnel working to close the reactor coolant system and containment building needed to continue their work. Announcements were subsequently made in an attempt to complete personnel accountability. However, because of the number of people working in the protected area, accountability was never satisfactorily completed. Several

attempts were made to account for those not in site emergency response facilities, and by 1:26 p.m., 4 hours and 6 minutes into the incident, 49 persons were yet to be accounted for.

At 10:15 a.m., 55 minutes into the incident, the incident was downgraded to an Alert after restoration of power to the 1A safety bus from the 1A emergency diesel generator and upon reestablishment of decay heat removal capability, using the 1A residual heat removal pump.

By 1 p.m., 3 hours and 40 minutes into the incident, plant conditions had stabilized. Offsite power had been restored to Unit 1 (two ac sources available) with decay heat removal via the residual heat removal system and with a second residual heat removal pump in standby. The Vogtle emergency director initiated a conference call with government officials in South Carolina, Georgia, and in Allendale, Barnwell, and Burke Counties, and with the Department of Energy's Savannah River Plant to discuss termination of the emergency. The emergency director also discussed termination with the Nuclear Regulatory Commission. Agreement was reached with all parties that the emergency would be terminated, which was done at 1:47 p.m., 4 hours and 27 minutes into the incident. All agencies were so notified at 1:56 p.m., 4 hours and 36 minutes into the incident, at which time the emergency was terminated.

10 FINDINGS AND CONCLUSIONS

10.1 Risk-Management Concepts Applied to Outage Planning and Scheduling During Shutdown

Plant configurations and equipment conditions were allowed to exist during the second refueling outage at Vogtle that resulted in an unnecessary reduction in safety. By planning, scheduling, and conducting outage activities based on the relative risk, the potential loss of the residual heat removal system during mid-loop operations and the potential for other risky plant configurations and conditions could have been limited without having a negative impact on the duration of the outage. Rather than doing this, the Vogtle staff relied on its technical specifications that contain few requirements for cold shutdown conditions.

10.2 Switchyard Administrative Control

10.2.1 Control of Activities in the Switchyard

At the time of the incident, the Vogtle staff had no restrictions or access controls prohibiting vehicles or equipment from entering and remaining inside the switchyard except that they be there on official business. Additional access controls, however, were implemented by the plant after the incident that were intended to ensure that activities are not permitted that could jeopardize operations in the future.

10.2.2 Control of Combustibles and Other Materials in the Switchyard

Although procedures did exist for the control of hazardous substances and waste within the Vogtle site boundary, there were no specific restrictions to control combustibles and other hazardous materials within the switchyard. The damage done by the fuel and lubricants truck in the Vogtle incident could have been more severe if electrical arcing had ignited the fuel on the truck. Losses of nonsafety power that could have resulted would have further complicated recovery of electrical power.

10.3 Power Availability During Shutdown Modes

10.3.1 Lack of Procedures for Bus Inter-connections

When one emergency diesel generator and one reserve auxiliary transformer were removed from service (two of four power sources to the safety buses), procedures did not exist that would provide guidance on how to use existing bus connections and other potentially available sources to restore power in an emergency where the preferred alternate or backup sources are not available. During the incident, personnel assigned to develop these procedures did not recognize that existing circuits which could be used to establish bus cross-ties required the energizing of the reserve auxiliary transformer which may be unavailable. The Vogtle loss of ac power procedures do not address shutdown conditions and were of little help during the incident.

10.3.2 Diesel Generator Lockout Following Shutdown

Following each of the two diesel generator shutdowns during the incident, the diesel generator locked out and could not be started by normal means because of the way in which the load sequencer circuitry and the diesel generator control circuitry interact when the diesel generator shuts down and an automatic start signal still exists. The interaction of the two control circuits for the wide variety of conditions that can exist is complex and was not understood by the plant operating staff.

10.3.3 Use of a "Missing Breaker" Arrangement to Prevent the Inter-connection of Safety Buses

A "missing breaker" arrangement is used at Vogtle to prevent the inadvertent interconnection of the two safety buses, or the simultaneous connection of a safety bus to both offsite power sources. However, this arrangement prevents live bus transfers between reserve auxiliary transformers, a condition which (1) limits the operator's flexibility for supplying continuous power to safety-related loads, and (2) requires additional emergency diesel generator starts to provide continuous power to the buses when making transfers. Because the 1B emergency diesel generator was out of service, the restoration of power from reserve auxiliary transformer 1B to safety bus 1B before the incident was delayed to prevent the need for a dead bus transfer. Restoration of reserve auxiliary transformer 1B could have prevented the incident, but one train of residual heat removal would be inoperable when the transfer was made, a configuration contrary to technical specification requirements for mid-loop operation. Other methods (e.g., key-lock switches) may allow flexibility for manipulating power sources and provide the same protection as the missing breaker arrangement for preventing the inadvertent connection of safety buses.

10.3.4 Plant Electrical Distribution System Design

The Nuclear Regulatory Commission (NRC) requires redundant protection when cross-ties exist between safety-related buses during reactor power operation to prevent a single electrical fault from degrading the power supplied to redundant trains of safety-related equipment. Typically, bus cross-ties include two circuit breakers in series that are interlocked and administratively controlled to ensure that the defense-in-depth provided by redundant safety-related equipment is not compromised. Cross-ties can also provide operators with flexibility when restoring power to safety-related equipment during emergency situations and therefore, also contribute to the defense-in-depth provided in a plant design. The economic costs required to provide protection against inadvertently cross-connecting buses should not discourage the installation of bus cross-ties. It is unclear whether the relative risks associated with bus cross-ties (i.e., potential degradation of redundant safety-related equipment when provided versus the unavailability of potential alternate sources of power when not provided) have been evaluated. A circuit breaker plus disconnects, when combined with administrative controls, may provide adequate protection at less cost than the double breaker arrangement

10.4 Diesel Generator Instrumentation and Control Systems

10.4.1 Pneumatic Control/Trip Sensor Reliability

Sensor calibration and test activities on diesel generator instrumentation and control systems prior to and subsequent to the incident recorded a multiplicity of sensor problems, particularly with respect to those for jacket water high temperature, lube oil low pressure, and lube oil high temperature. Sensors were found to have leaks, to stick in the tripped position, to have a sluggish response, and to have significantly changed trip set-points several weeks after calibration. Subsequent investigation determined that foreign materials in the jacket water temperature sensors (i.e., pipe thread sealant compound and metal shavings from the sensor-to-air tubing threaded connections) prevented proper operation and were the most likely cause for the unexpected diesel generator trips. These sensors are standard parts on Transamerica Delaval diesel generators at nuclear plants.

10.4.2 Diesel Generator Start on Under-voltage

An under-voltage start of the emergency diesel generator puts the engine in a "normal" start and run mode. In this mode all engine protective trips are active. During the incident, the diesel generator started twice on under-voltage and shut down each time because of false protective trips. In an "emergency" start and run mode, only the most crucial protective trips are active. Diesel generators are less susceptible to false trips caused by malfunctioning sensors when they are in an emergency operating mode. The diesel generator start logic at Vogtle has been modified since the incident to change the bus under-voltage start from a normal start to an emergency start. In addition, the diesel generator trip logic has been modified to bypass the jacket water high temperature trip function on an emergency start.

10.4.3 Design for Emergency Diesel Generator Trip Identification

Design deficiencies were noted at the local and control room diesel generator panels and discrepancies were noted between the panels. The design of the first out alarm feature was not useful in identifying the causes of the diesel generator annunciator trips. Numerous nuisance alarms were received for each diesel trip, contributing to operator confusion in identifying the cause of the trip. In addition, the design did not include provisions for recording diesel generator trip alarms. As a result of these weaknesses, the operators had difficulty diagnosing the causes of the diesel generator trips. The operator training program and existing procedures did not provide the operators with adequate information regarding the operation of the diesel generator control and annunciator systems.

10.5 Coping With the Loss of the Residual Heat Removal System

10.5.1 Existing Guidance

Generic Letter 88-17 provided extensive guidance for improving the capability to respond to a loss of residual heat removal (RHR) systems, but this guidance had not been fully implemented at Vogtle. For example, the lessons learned from Diablo Canyon were incompletely addressed in training and procedures. Containment building closure and level instrument error due to blocking the pressurizer surge line with water were incompletely addressed.

10.5.2 Immediate Response to Lessons Learned from the Vogtle Incident

A review of the loss of RHR systems indicated that limited guidance was provided for dealing with the results of loss of electrical power. The Vogtle incident established that maintaining core cooling without electric power is not adequately addressed in the loss of RHR system procedures.

10.5.3 Understanding Shutdown Thermohydraulic Phenomena and Behavior

The Team evaluated existing analysis and understanding at Vogtle and concluded that areas such as gravity feed control, prevention of reactor coolant system boiling, level instrument response, control of boiling by gravity feed, and reflux cooling were incompletely addressed in Vogtle's analyses, training, and procedures. This conclusion was confirmed by interviews with plant personnel involved in responding to the Vogtle incident.

10.5.4 Containment Building Equipment Hatch Closure

The critical path (i.e., activity of longest duration) in establishing containment building integrity during the Vogtle incident was closing the equipment hatch. Procedures for an expedited closure of the containment building equipment hatch did not exist. Generic Letter 88-17 recommended that procedures and administrative controls for containment building closure prior to the time at which uncovering the core could occur be in place or that licensees should either not enter the applicable condition or should maintain a closed containment building. Vogtle took 79 minutes to close the equipment hatch. Their analysis stated they had 57 minutes in which to close the hatch for the bounding case. Vogtle did not demonstrate that they could close the hatch within the time available in their own bounding case assessment.

Vogtle's analysis and procedures focused on closing the containment building before the core becomes uncovered. The procedures instruct the operator to initiate closure if the core exit thermocouples reach 200 °F. The Vogtle analysis measures time from when the residual heat removal system is lost. Further, the analyses do not adequately address containment building habitability.

10.5.5 Loss of Residual Heat Removal System Procedure

The Vogtle loss of RHR system procedure provided some guidance regarding response to a loss of the RHR system and to reactor coolant system temperature and level indications. Although containment building closure and gravity feed of water from the refueling water storage tank to the reactor coolant system are identified, the guidance is sometimes incomplete, incorrect, and difficult to follow.

10.5.6 Failure of Temporary Thimble Tube Seals

The possibility of temporary thimble tube seal failure from overpressurization in the reactor coolant system has not been recognized or evaluated, and the resulting leak rate may be significant. Vogtle's procedures do not recognize this possibility when providing operator guidance for pressure control.

10.5.7 Valve Inspections Requiring Mid-Loop Conditions

At present, the disassembly of some check valves requires that the reactor coolant system water level be drained to a mid-loop condition. Alternatives to full-flow testing or disassembly and inspection to determine check valve operability may exist and, if this is the case, could decrease the need for mid-loop operation.

10.5.8 Reactor Coolant System Configuration Control

There was no procedure or training that addressed changing the reactor coolant system configuration in response to a loss of the RHR system event. Consequently, the Vogtle operators followed their instincts and elected to close all reactor coolant system openings except for the pressurizer manway. This plan was not properly implemented when the pressurizer manway was already closed.

There are both benefits and liabilities to having an intact reactor coolant system pressure boundary during a loss of the residual heat removal system. These have not been evaluated, nor do the analyses exist to permit such an evaluation. The discovery of the potential thimble tube seal failure emphasizes the importance of including boundary breach locations based on actual hardware.

10.6 Emergency Preparedness

10.6.1 Applicability of Emergency Classification Levels to the Conditions of Refueling or Cold Shutdown

NUREG-0654 does not provide adequate classification guidance for loss of power and loss of RHR system events during cold shutdown operation. Based on NUREG-0654, the highest classification for an event similar to Vogtle's would be an Alert. This classification may not convey the seriousness of the situation that could include complete

loss of the residual heat removal system with the containment building open, the reactor coolant system open, and the reactor coolant system inventory reduced, making boiling possible within 10 to 20 minutes.

10.6.2 Inconsistent Implementation of NUREG-0654 Emergency Classification Guidance for Loss of Power Events

Emergency classification guidance for loss of power events in NUREG-0654 is ambiguous and inconsistent. The ambiguous guidance, combined with inconsistent review and approval of licensee classification procedures by NRC, has led to inconsistent implementation. A sampling of classification procedures from 12 sites other than Vogtle showed that the classification of a similar loss-of-coolant incident at those sites could range from "no classification at all" to a Site Area Emergency.

10.6.3 Evacuation and Accountability of Onsite Personnel for Emergencies During Outages

It is not clear that the guidelines established in NUREG-0654 for the evacuation and accountability of site personnel adequately considered the presence of large numbers of people onsite and the fact that there may be a valid need for significant numbers of maintenance personnel to continue working in direct response to the emergency without going first to the Operations Support Center where they would be accounted for.

10.6.4 Notification of State and Local Authorities During Emergencies

During this incident, Vogtle personnel did not meet the 15-minute notification goal for the emergency response authorities in the plume exposure emergency planning zone (EPZ) because of the lack of power to the emergency notification network in the control room and because of some training and procedural weaknesses.

10.6.5 Notification of the NRC During Emergencies

During this incident a problem with the telephone system between Vogtle and the NRC Operations Center resulted in numerous lost connections. This occurred with both the commercial phone and the Emergency Notification System (ENS) telephone from the site and significantly slowed communications with Vogtle. The problems appear to be located in the telephone circuits at Vogtle or in the vicinity; however, the problem has not yet been localized and corrected.

10.6.6 NRC Standby Mode During Incident Response

NRC did not go to a Standby mode until 1 hour after initial notification of the incident. The delay had no significant effect on NRC's response to the Vogtle incident because it occurred during the day and ample qualified staff were available to respond to the incident, including executing those tasks associated with Standby, i.e., completing notifications, responding

to inquiries, and completing liaison functions. At the time of initial notification safety power had already been restored to one of the safety buses, and therefore the situation was improving. From the generic standpoint, however, not placing the NRC in Standby for an Alert, Site Area Emergency, or General Emergency, as prescribed by the Incident Response Plan, may have the following negative affects on the response:

- A misunderstanding could exist among NRC response personnel as to what tasks should be conducted at that point in the response.
- Not placing NRC in Standby could be interpreted to mean that NRC does not consider the incident to be as serious as the licensee's classification indicates.
- Outside agencies and the public would not be aware of the level of response being undertaken by the NRC if the Standby tasks were being conducted, but the agency had not officially gone to a Standby status.
- Not placing NRC in Standby when appropriate could unintentionally affect the level of response of other agencies to the incident.

10.7 Feedback to Industry Based on Operating Experience

10.7.1 Lack of Guidance on Loss of the Residual Heat Removal System During Mid-loop Operations Because of Loss of Power to Safety Buses

Guidance over a 10-year period has been provided by the NRC and the Institute of Nuclear Power Operations (INPO) to the industry for preventing and mitigating loss of decay heat removal incidents. The guidance provided was concerned with loss of the residual heat removal system and was not explicitly focused on ensuring that an adequate number of sources of power are available to energize emergency buses during operations with reduced reactor coolant system inventory.

10.7.2 Lack of Guidance on Loss of Offsite Power During Cold Shutdown Operations

Most guidance provided by NRC and INPO to the industry related to loss of offsite power incidents during cold shutdown operation primarily focused on preventing inadvertent reactor trips of the operating unit. Over the past 10 years, only four of these operating experience documents focused on issues related to loss of power during shutdown conditions. The guidance to the industry has not reflected the frequency of loss of offsite power incidents that have occurred with the plant in cold shutdown when one emergency power source failed to function and the other emergency power source was out of service.

10.7.3 Diesel Generator Trip Sensor Operating Experience

Both NRC and INPO operating experience documents have addressed the need for preventive maintenance programs that determine causes of failures for emergency diesel generators. Vogtle has experienced about twice as many trip sensor failures as the rest of the industry has reported. Vogtle did not provide the failure data to the Nuclear Plant Reliability Data System so that their experience could be easily compared to that of other plants. When the diesel generator manufacturer published information on similar failures experienced at the other plants, Vogtle personnel did not analyze the failures of trip sensors they had experienced. In addition, 30 failures of these sensors occurred during the 6-month period after the operating experience information was provided to the plant.

10.7.4 Assimilation and Dissemination of Operating Experience Guidance

Between 1980 and 1989, 54 partial or total loss-of-offsite power events occurred while plants were in cold shutdown conditions. In some of these events, power was lost to safety buses. During the same period, 46 loss-of-residual-heat-removal-system events occurred while plants were operating with the water level at mid-loop. NRC and INPO provided the industry with lessons learned from the loss of offsite power events in 16 operating experience documents and from the loss of the residual heat removal system events at mid-loop in 26 operating experience documents. The number and pattern of some event types, such as loss of offsite power during shutdown, have not been evaluated by NRC and INPO and appropriate guidance has not been provided to focus on the generic implications that can be developed from the existing published operating experience.

10.8 Technical Specifications for Reduced Inventory Operations

10.8.1 Technical Specification Bases

Technical specifications which control nonpower operations, especially reduced inventory operation, have been developed with little analysis or safety consideration. Situations encountered during power operation do not bound situations that could occur during reduced inventory operation. Generally, single-failure criteria have not been applied to shutdown and operations. This area may merit further consideration.

10.8.2 System Interrelationships in Technical Specifications

In general, the interrelationships of important systems are not considered in technical specifications. With the exception of the residual heat removal system, technical specification allowable conditions for various systems (e.g., electrical sources and distribution, the containment building) do not recognize vulnerabilities allowed by the status of other systems, or those created by reactor coolant system (RCS) integrity, RCS water inventory, or RCS decay heat generation rate conditions. Technical specification limiting conditions for operation do not preclude increases in vulnerability during certain phases of nonpower operations.

10.8.3 Containment Building Integrity

Technical specifications do not require containment building integrity during cold shutdown and refueling operations unless core alterations are in progress. They do not require containment building integrity during reduced inventory or with reduced electrical sources.

10.8.4 Electrical Distribution

Technical specifications effectively require only one-half of the electrical sources and trains of electrical equipment to be in service during Modes 5 and 6 compared with those required during Modes 1, 2, 3, and 4. They do not require additional electrical sources during reduced inventory operation.

10.8.5 Makeup Water Sources for the Reactor Coolant System

The capability to add water to the reactor coolant system is reduced in Modes 5 and 6 relative to Modes 1, 2, 3, and 4. Technical specifications do not recognize increased vulnerabilities and the possible increased need to add water during reduced inventory operation.

10.8.6 Decay Heat Generation Rate

Technical specifications do not impose a required shutdown period or other limit (e.g., decay heat level) before reduced inventory operations may be conducted.

10.8.7 Reactor Coolant System Cooling

Requirements for residual heat removal system operability and flow rate vary based on reactor coolant system water level and mode. These are the only nonpower technical specifications which vary within mode. However, they may increase the potential for residual heat removal pump cavitation by requiring a minimum residual heat removal pump flow rate which may be unnecessarily high.