C.5 LER No. 250/94-005

Event Description: Load Sequencers Periodically Inoperable

Date of Event: November 3, 1994

Plant: Turkey Point 3 and 4

C.5.1 Summary

During a Unit 4 Integrated Safeguards Test, the 3A sequencer failed to respond to the opposite unit's safety actuation signal. Troubleshooting resulted in the discovery of an error in the sequencer software logic that could prevent each of the four Turkey Point sequencers from responding to a safety actuation signal. As a result of the software error, each sequencer was unavailable one-fourth of the time to respond to automatic safety actuation signals from its own train and one-sixteenth of the time to respond to automatic signals from the other unit during both automatic self-testing and manual testing. Unavailability of each sequencer would prevent the automatic actuation of safety-related equipment associated with that train including the high head safety injection (HHSI) and residual heat removal (RHR) pumps.

The estimated increase in core damage probability for this event for a 1-year period is 1.8×10^{-6}, over a nominal value for the same period of 9.5×10^{-5}. This value is applicable to each unit.

C.5.2 Event Description

On November 3, 1994, Turkey Point Unit 3 was operating at 100% power, and Unit 4 was in Mode 5 during a refueling outage. During the Unit 4 Integrated Safeguards Test, the 3A sequencer failed to respond to the opposite unit's safety actuation signal. Troubleshooting resulted in the discovery of an error in the sequencer software logic that could prevent each sequencer from responding to a safety actuation signal. The error impacted the Turkey Point 3 sequencers since November 1992 and the Turkey Point 4 sequencers since May 1993.

The Turkey Point design utilizes four sequencers, one for each train at each unit. The sequencers are programmable logic controller (PLC)-based cabinets that use a PLC for bus stripping and logic control. The sequencers are designed to respond to losses of offsite power (LOOPs), loss-of-coolant accidents (LOCAs), and combined LOOP/LOCA events. The sequencers start the diesel generators and sequentially load safety-related equipment required to respond to the initiating event. Each sequencer responds to safety actuation signals associated with its train plus signals from the opposite unit.

Each sequencer is provided with manual and automatic self-test capabilities. The automatic test mode is normally in operation. In the automatic test mode, the sequencer continually tests the input cards, output cards, and output relay coils and exercises the program logic. The automatic self-test cycles through 15 of 16 possible sequencer test steps. The test steps start roughly an hour apart and individually take about 10 s to complete. There is 1 h during which no testing takes place. The complete automatic test cycle, therefore, takes about 16 h and then begins again. The sequencer is designed to abort the manual and automatic test modes in response to a valid input. If a valid input signal is received during sequencer testing, the testing stops, the test signal clears, and the inhibit signal, if present, is supposed to clear. The valid signal is then allowed to sequentially energize the output relays for the associated safety-related equipment.

The 3A sequencer had dropped out of the automatic self-test without alarming, indicating that it had received a valid input signal. During troubleshooting, the input light emitting diode (LED) for the 4A safety actuation signal was found to be lit, indicating the signal was still present. The 3A sequencer response should have been to start the 3A HHSI pump. However, the pump failed to start because it did not receive a start signal from the sequencer.

A software design error was discovered that inhibited the 3A HHSI pump start signal even though a valid input signal was present. The design error was found to affect all sequencers during both manual and automatic testing in 5 of the 16 test steps. If a valid input signal was received 15 s or later into one of the hour-long test step periods, the test signal cleared as intended, but the inhibit signal was maintained by means of latching logic. This latching logic is established by the test signal but could be maintained by the process input signal if it arrived prior to removal of the test signal.

This software logic error was introduced during the detailed logic design phase of the software development. The error was not discovered during the validation and verification (V&V) process because the response to valid inputs was not tested during all test sequences of the testing logic. In four loading sequence tests, the error prevented the sequencer from responding to a valid safety actuation signal on the same train. In one other loading sequence test, the error prevented the sequencer from responding to a valid safety actuation signal on the opposite unit. This software error did not impact response to LOOP or a combined LOOP and LOCA; only safety actuation with offsite power available was affected. The logic error also did not affect sequencer operation with the test selector switch in the "off" position.

A detailed review of the sequencer software resulted in the discovery of one other error in the software, which was independent of the test mode. A condition was identified that would have prevented the automatic start of the containment spray pumps. The condition would occur when a hi–hi containment pressure signal is received by the sequencer during a 60-ms time window beginning 12.886 s after receipt of a LOCA signal or 28.886 s after receipt of a LOOP/LOCA signal. This error does not impact core damage sequences and was not addressed in this analysis.

C.5.3 Additional Event-Related Information

For non-LOOP events, each sequencer sends start signals to the following equipment associated with its train: one RHR pump, one HHSI pump, two intake cooling water pumps, two emergency containment cooler fans, two component cooling water pumps, and two emergency containment filter fans. Some equipment may already be in operation and would not be affected by a sequencer failure.

Turkey Point has four HHSI pumps, one per train for each unit. All four trains are normally cross-connected at the discharge of the pumps. Each HHSI pump is capable of providing 50% of the required injection; two of the four pumps are, therefore, required for high-pressure injection success following a small-break LOCA. To meet single failure criteria for a safety actuation, each sequencer signals its associated HHSI pump to start, and the opposite unit's sequencers signal their associated HHSI pumps to start. For example, a safety actuation signal on Unit 3, Train A, signals the 3A sequencer and both of the Unit 4 sequencers. With no equipment failures, all four HHSI pumps will respond to a safety actuation signal on either unit. Other equipment provided for each unit, including the two RHR pumps, is only started by its associated sequencer.

C.5.4 Modeling Assumptions

This event was modeled as an unavailability of HHSI and RHR pump automatic actuation for LOCA-related sequences during a 1-year period. Assuming the units were at power 70% of the time, an unavailability of 6132 h is estimated.

The Accident Sequence Precursor (ASP) Program typically considers the potential for core damage following three postulated offsite-power-available pressurized water reactor (PWR) initiating events: transient, small-break LOCAs, and steam generator tube rupture (SGTR). For each of these initiating events, unavailability of high-pressure injection, when required to make up inventory lost from the reactor coolant system, is assumed to result in core damage. Two additional initiating events also exist that are impacted by the unavailability of the HHSI and RHR pumps: medium- and large-break LOCAs. For both of these initiating events, unavailability of low-pressure injection is assumed to result in core damage.

The significance of an unavailability such as this event is estimated in the ASP Program in terms of the increase in core damage probability during the unavailability period. Since a nonrecoverable failure of multiple sequencers will fail high- and low-pressure injection, and, since unavailability of high- and low-pressure injection following a LOCA

proceeds to core damage, the significance of this event can be estimated directly from the change in high- and low-pressure injection failure probabilities due to the sequencer software error and the probability of a small-, medium-, and large-break LOCA in the 6132-hour unavailability period.

Small-break LOCA. Small-break LOCA initiating events, SGTRs, and transient-induced LOCAs (primarily stuck-open relief valves for non-LOOP transients) were considered small-break LOCAs in this analysis. The frequencies of these three events, based on data used in the ASP models, are 1.4×10^{-8}/h (transient induced LOCA), 4.7×10^{-7}/h [small-break LOCA initiating events (spurious relief valve lifts, reactor coolant pump seal failures)], and 1.6×10^{-6}/h (SGTRs). Summing these values results in an overall small-break LOCA frequency of 2.1×10^{-6}/h. For the 6132-hour unavailability period, the probability of a small-break LOCA is 1.3×10^{-2}.

For a small-break LOCA, two of four HHSI pumps provide injection success; failure of three of the four pumps will, therefore, fail high-pressure injection. Since the software error did not affect sequencer response to LOOPs, only single-unit initiating events are of concern in the analysis (if LOOP response was affected, then potential dual-unit events such as a severe weather-related LOOP would also have to be considered). Assume the small-break LOCA occurs at Unit 3. The probability of the sequencers failing to actuate the four HHSI pumps is 0.25 for HHSI pumps 3A and 3B (the sequencers would not respond to a valid signal on the same train during 4 of the 16 loading sequence tests) and 0.0625 for HHSI pumps 4A and 4B (the sequencers would not respond to a valid signal from the opposite unit during one of the 16 loading sequence tests). The probability of three of the four pumps failing is estimated by considering the pump failure combinations that can result in injection failure:

$$p(3A) \times p(3B) \times p(4A) + p(3A) \times p(3B) \times p(4B) +$$

$$p(3A) \times p(4A) \times p(4B) + p(3B) \times p(4A) \times p(4B) = 9.8 \times 10^{-3}.$$

Consideration of the sequencer testing process indicates that an assumption that the sequencers fail independently is reasonable. If the testing of the two sequencers on each unit is synchronized, the increased HHSI failure probability is

$$0.25 \times 1.0 \times 0.0625 + 0.25 \times 1.0 \times 0.0625 + 0.25 \times 0.0625 \times 1.0 + 0.25 \times 0.0625 \times 1.0 = 6.3 \times 10^{-2},$$

using the same approach as in the last paragraph. If the testing of the four sequencers were somehow synchronized, the increased HHSI failure probability would be zero, since the test step that prevents response from the opposite unit is different from the steps that prevent response on the same train. The potential impact of synchronized testing of both sequencers on an individual unit was addressed as a sensitivity analysis.

For a small-break LOCA, manual initiation of safety injection (SI) within 30 min of the LOCA is assumed to result in injection success. Assuming 5 min to reach the procedure step to verify SI, 25 min would be available for operator action. The probability of failure to recover SI due to operator error was estimated by assuming that the failure probability can be represented as a time-reliability correlation (TRC) as described in *Human Reliability Analysis* (E. M. Dougherty and J. R. Fragola, John Wiley and Sons, New York, 1988). Operator response was assumed to be rule-based and without hesitancy. For the 25-min period, a failure probability of 1.8×10^{-4} is estimated.

The increase in core damage probability for small-break LOCAs resulting from the sequencer software error is, therefore,

1.3×10^{-2}(probability of a small-break LOCA in the 6132-h period) ×

9.8×10^{-3}(probability of HHSI actuation failure due to the software error) ×

1.8×10^{-4}(probability that the operators fail to manually initiate SI prior to core damage)

$= 2.2 \times 10^{-8}$.

Medium- and large-break LOCAs. The analysis of postulated medium- and large-break LOCAs follows the same approach as a small-break LOCA. The frequency of medium- and large-break LOCAs is estimated to be 1×10^{-3}/year

and 2.7×10^{-4}/year, respectively (see *Analysis of Core Damage Frequency: Internal Events Methodology*, NUREG/CR-4550, Vol. 1, Rev. 1, Table 8.2-4 and Appendix H to this report). Mitigation of both medium- and large-break LOCAs requires low-pressure safety injection (LPSI) success. Two RHR pumps are available for injection, and one of two provides success. Since the two RHR pumps are actuated only by their same-train sequencers, an actuation failure probability of $0.25 \times 0.25 = 0.0625$ is estimated.

Assuming manual initiation of SI within 20 min of a medium-break LOCA provides injection success (this value is consistent with *Analysis of Core Damage Frequency: Surry, Unit 1, Internal Events*, NUREG/CR-4550, Vol. 3, Rev. 1, Part 1, Table 4.8-4), an operator failure probability of 2.2×10^{-3} is estimated, using the same approach as described for small-break LOCAs.

For a large-break LOCA an operator failure probability of 0.095 is estimated. This value was developed from simulator data provided in the licensee event report (LER) using the same TRC approach that was used to estimate operator failure probabilities for small- and medium-break LOCAs. The data provided in the LER were assumed to represent unburdened response; their standard deviation was revised to reflect burdened response as described on p. 127 of *Human Reliability Analysis*. The allowed response time was assumed to be 7.1 min, as specified in Appendix D.4 of NUREG/CR-4550, Vol. 3, Rev. 1. This is the time to core uncovery estimated using the MARCH code during source term calculations performed in 1984.

These estimates result in the following increase in core damage probability for medium- and large-break LOCAs:

1.0×10^{-3}(probability of a medium-break LOCA in a 1-year period (6132 at-power hours) ×

0.0625(probability of LPSI actuation failure due to the software error) ×

2.2×10^{-3}(probability that the operators fail to manually initiate LPSI)

$= 1.4 \times 10^{-7}$ (medium-break LOCA),

and

2.7×10^{-4} (probability of a large-break LOCA in a 1-year period (6132 at-power hours) ×

0.0625 (probability of LPSI actuation failure due to the software error) ×

0.095 (probability that the operators fail to manually initiate LPSI)

$= 1.6 \times 10^{-6}$ (large-break LOCA).

C.5.5 Analysis Results

Combining the probability estimates for small-, medium-, and large-break LOCAs results in an overall increase in core damage probability for the sequencer software error over a 1-year period of 1.8×10^{-6}, contributed almost entirely by postulated large-break LOCAs. This value is applicable to each unit. The dominant core damage sequence for the event involves a postulated large-break LOCA and failure of low-pressure injection. This sequence is highlighted in Figure C.5.1.

A greater than usual uncertainty is associated with this estimate. It is based on an estimated frequency of a large-break LOCA (no large-break or medium-break LOCAs have occurred), an estimated time to core uncovery developed in conjunction with source term calculations (there is large uncertainty in this estimated time), and assumptions regarding operator actions following a large-break LOCA.

The nominal core damage probability over a 1-year period estimated using the ASP models for Turkey Point is approximately 9.5×10^{-5}. The failed sequencers increased this probability by 2% to 9.7×10^{-5}. This value is the conditional core damage probability for the 1-year period in which the sequencers were degraded.

For most ASP analyses of conditions (equipment failures over a period of time during which postulated initiating events could have occurred), sequences and cutsets associated with the observed failures dominate the conditional core damage probability (the probability of core damage over the unavailability period, given the observed failures). The increase in core damage probability because of the failures is therefore essentially the same as the conditional core damage probability, and the conditional core damage probability can be considered a reasonable measure of the significance of the observed failures.

For this event, however, sequences unrelated to the degraded sequencers dominate the conditional core damage probability estimate. The increase in core damage probability given the degraded sequencers, 1.8×10^{-6}, is, therefore, a better measure of the significance of the sequencer problems.

If the sequencer testing was synchronized at each unit, the actuation failure probability for the HHSI pumps would increase to 6.3×10^{-2} as described in the modeling assumptions. The failure probability for low-pressure injection actuation would also increase to 0.25. These failure probabilities were used in a sensitivity analysis to estimate the potential impact if the testing were synchronized. The resulting estimated increase in core damage probability is 7.1×10^{-6}, again primarily from large-break LOCAs.

C.5.6 Reference

1. LER 250/94-005, Rev. 1, "Design Defect in Safeguards Bus Sequence Test Logic Places Both Units Outside the Design Basis," February 9, 1995.

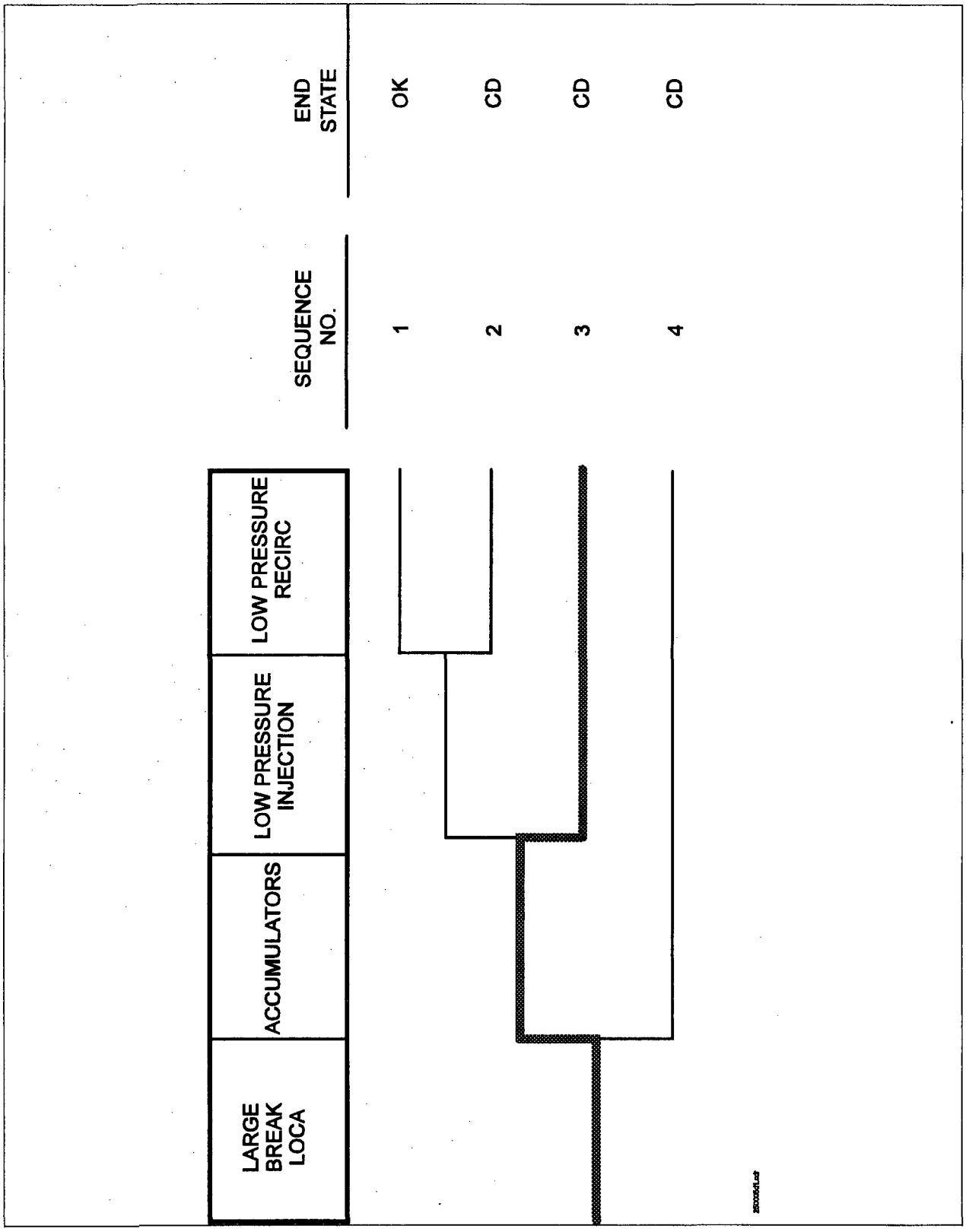

Figure C.5.1. Dominant core damage sequence for LER 250/94-005.