PRIORITY 1
(ACCELERATED RIDS PROCESSING)

REGULATORY INFORMATION DISTRIBUTION SYSTEM (RIDS)

ACCESSION NBR:9502220392 DOC.DATE: 95/02/09 NOTARIZED: NO DOCKET #
FACIL:50-250 Turkey Point Plant, Unit 3, Florida Power and Light C 05000250
AUTH.NAME AUTHOR AFFILIATION
MOWREY,C.L. Florida Power & Light Co.
PLUNKETT,T.F. Florida Power & Light Co.
RECIP.NAME RECIPIENT AFFILIATION

SUBJECT: LER 94-005-01:on 941103,design defect found in safeguards bus sequencer test logic,placing facility outside design basis.Design mods to eliminate software logic problems will be implemented during next refueling outages.W/950209 ltr.

DISTRIBUTION CODE: IE22T COPIES RECEIVED:LTR 1 ENCL 1 SIZE: 19
TITLE: 50.73/50.9 Licensee Event Report (LER), Incident Rpt, etc.

NOTES:

	RECIPIENT ID CODE/NAME	COPIES LTTR	COPIES ENCL	RECIPIENT ID CODE/NAME	COPIES LTTR	COPIES ENCL
	PD2-2 PD	1	1	CROTEAU,R	1	1
INTERNAL:	AEOD/SPD/RAB	1	1	AEOD/SPD/RRAB	1	1
	FILE CENTER 02	1	1	NRR/DE/ECGB	1	1
	NRR/DE/EELB	1	1	NRR/DE/EMEB	1	1
	NRR/DISP/PIPB	1	1	NRR/DOPS/OECB	1	1
	NRR/DRCH/HHFB	1	1	NRR/DRCH/HICB	1	1
	NRR/DRCH/HOLB	1	1	NRR/DRSS/PRPB	2	2
	NRR/DSSA/SPLB	1	1	NRR/DSSA/SRXB	1	1
	RES/DSIR/EIB	1	1	RGN2 FILE 01	1	1
EXTERNAL:	L ST LOBBY WARD	1	1	LITCO BRYCE,J H	2	2
	NOAC MURPHY,G.A	1	1	NOAC POORE,W.	1	1
	NRC PDR	1	1	NUDOCS FULL TXT	1	1

NOTE TO ALL "RIDS" RECIPIENTS
PLEASE HELP US TO REDUCE WASTE! CONTACT THE DOCUMENT CONTROL DESK, ROOM P1-37 (EXT 504-2083) TO ELIMINATE YOUR NAME FROM DISTRIBUTION LISTS FOR DOCUMENTS YOU DON'T NEED!

FULL TEXT CONVERSION REQUIRED
TOTAL NUMBER OF COPIES REQUIRED: LTTR 26 ENCL 26

A04

PRIORITY 1 DOCUMENT

FPL

FEB 09 1995
L-95-038
10 CFR 50.73

U. S. Nuclear Regulatory Commission
Attn: Document Control Desk
Washington, D. C. 20555

Gentlemen:

Re: Turkey Point Units 3 and 4
Docket No. 50-250, 50-251
Reportable Event: 94-005-01
Design Defect in Safeguards Bus Sequencer Logic Timing Places Both Units Outside the Design Basis

The attached revised Licensee Event Report 250/94-005-01 is being provided in accordance with 10 CFR 50.73(a)(2)(ii), (a)(2)(v), (a)(2)(vii), AND 10 CFR 21.

If there are any questions, please contact us.

Very truly yours,

T. F. Plunkett
Vice President
Turkey Point Plant

TFP/CLM/cm

enclosure

cc: Stewart D. Ebneter, Regional Administrator, Region II, USNRC
Thomas P. Johnson, Senior Resident Inspector, Turkey Point Plant, USNRC

IE22

LICENSEE EVENT REPORT (LER)

FACILITY NAME (1)	DOCKET NUMBER (2)	PAGE (3)
TURKEY POINT UNITS 3 AND 4	05000250	1 OF 18

TITLE (4) DESIGN DEFECT IN SAFEGUARDS BUS SEQUENCER TEST LOGIC PLACES BOTH UNITS OUTSIDE THE DESIGN BASIS

EVENT DATE (5)			LER NUMBER(6)			RPT DATE (7)			OTHER FACILITIES INV. (8)	
MON	DAY	YR	YR	SEQ #	R#	MON	DAY	YR	FACILITY NAMES	DOCKET # (S)
11	03	94	94	005	01	02	09	95	TURKEY POINT UNIT 4	05000251

OPERATING MODE (9)	1/5	10 CFR 50.73(a)(2)(ii), (a)(2)(v), (a)(2)(vii), 10 CFR 21
POWER LEVEL (10)	100/0	

LICENSEE CONTACT FOR THIS LER (12)

	TELEPHONE NUMBER
C. L. Mowrey, Licensing OEF Engineer/Analyst	305-246-6204

COMPLETE ONE LINE FOR EACH COMPONENT FAILURE DESCRIBED IN THIS REPORT (13)

CAUSE	SYSTEM	COMPONENT	MANUFACTURER	NPRDS?	CAUSE	SYSTEM	COMPONENT	MANUFACTURER	NPRDS?
B	JE	34	A160	Y					

SUPPLEMENTAL REPORT EXPECTED (14)	EXPECTED SUBMISSION DATE (15)	MONTH	DAY	YEAR
NO ☒ YES ☐				
(If yes, complete EXPECTED SUBMISSION DATE)				

ABSTRACT (16)

On November 3, 1994, Turkey Point Unit 3 was in Mode 1 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 Unit 4 Safety Injection signal. A defect was found in the sequencer software logic which, for a limited period of time, could inhibit any or all of the four sequencers from responding to specific valid signals. The defect only affects the sequencers during manual or automatic testing. The sequencers were installed in late 1991.

Monthly manual testing of the sequencer has been resumed. Front panel visual examinations are being performed every 8 hours, and internal visual examinations are being performed every 24 hours. A permanent repair to the software logic is being evaluated. Independent consultants performed an assessment of the existing sequencer design, software design, and the Validation and Verification process. One other software error involving Containment Spray (CS) pump autostart was discovered, and determined to have minimal safety significance. The CS system remains operable.

I. DESCRIPTION OF THE EVENT

On November 3, 1994, Turkey Point Unit 3 was operating in Mode 1 at 100% power, and Unit 4 was in Mode 5 during a refueling outage. During the Unit 4 Integrated Safeguards Test, a failure of the 3A sequencer [JE:34] to respond to the opposite unit's Safety Injection (SI) signal occurred. Troubleshooting resulted in the discovery of a defect in the sequencer software logic which, under certain conditions, could inhibit the sequencer from responding to a valid emergency signal. The defect manifested itself in the failure of the 3A High Head Safety Injection (HHSI) pump [BQ:p] to start. Turkey Point has four HHSI pumps; one per train, per unit. Each HHSI pump is capable of providing 50 percent of system requirements, therefore two of the four are required to mitigate the consequences of accidents analyzed in the Updated Final Safety Analysis Report (UFSAR). In order to meet single failure criteria, each sequencer signals its associated HHSI pump to start, and the opposite unit's sequencers signal their associated HHSI pumps to start. For example, an SI 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 an SI signal on either unit.

The software logic defect is limited to the test function, but the defect is common to all four sequencers (one sequencer per train, per unit). The design intent of the sequencers is such that should a "real" emergency signal occur while the sequencer is being tested, the test signal clears, allowing actuation of the Engineered Safety Features controlled by the sequencer.

Because the sequencers would not have responded properly to an SI signal as designed, Turkey Point Units 3 and 4 have been operating outside their design basis. This condition was reported to the NRCOC at 1609 on November 3, 1994, in accordance with 10CFR50.72(b)(ii)(B).

The detailed review of the sequencer software, described in Corrective Action #6, resulted in the discovery of one other error in the software, which is independent of the test mode. A potential condition was identified which, for a remote set of circumstances, would preclude the automatic start of the Containment Spray (CS) pumps [BE:p]. The condition identified occurs when the Hi-Hi Containment Pressure (HHCP) signal is received by the sequencer during an approximate 60 millisecond (ms) time window just prior to the end of sequencer load block 3 for Loss of Coolant Accident (LOCA) or Loss of Offsite Power coincident with LOCA (LOOP/LOCA) events. The sequencer is designed to autostart the CS pumps 11 to 13 seconds after an SI signal (without LOOP) if the HHCP signal is present or at or after 44 seconds under conditions where the HHCP signal occurs more than 13 seconds after receipt of the SI signal. For a LOOP/LOCA, these times are shifted by the bus stripping and EDG start delay of approximately 16 seconds. Thus the 60 ms window occurs 12.886 to 12.945 seconds after receipt of an LOCA signal, or 28.886 to 28.945 seconds after receipt of a LOOP/LOCA signal.

Although Turkey Point is licensed to accommodate a LOCA with or without a concurrent LOOP, the sequencer was designed to accommodate non-concurrent LOOP/LOCA sequences as well. As a result, for certain non-concurrent events, a Main Steam Line Break or a Small Break LOCA (but large enough to cause a HHCP signal) can also create conditions under which this error may manifest itself.

Automatic CS pump start actually involves two HHCP signals; one via the sequencer logic as described above, and one directly from Engineered Safety Features Actuation System (ESFAS) relay [JE:44]. Because of the minimum pulse required to assure CS pump breaker [BE:bkr] closure, and a potential relay race with a CS pump start permissive from ESFAS, the CS pump breaker may not receive a close signal of sufficient duration to assure breaker closure. The identified condition is unique to the start of the CS pump because the CS pump start signal duration decreases as the postulated receipt of a HHCP signal approaches the end of load block 3. All other sequenced equipment receives a start pulse of fixed duration, either 2 or 5 seconds. This condition was determined to be not significant, in part because the manual start capability of the CS pump is not affected (and is adequately proceduralized), and in part because the probability of occurrence of the condition is lower than the probability of a common-mode failure of both trains of containment spray. The significance of the condition is discussed further in Section III.

SEQUENCER DESIGN BASIS AND FUNCTIONAL REQUIREMENTS

Each of the four sequencers, 3C23A-1, 3C23B-1, 4C23A-1, and 4C23B-1, is associated with a given train (3A, 3B, 4A, and 4B, respectively). They are designated Class 1E, Seismic Category I, since their operation is required for safe shutdown of the reactor in the event of a Loss of Offsite Power (LOOP) and to mitigate the consequences of a design basis accident.

The sequencers are Programmable Logic Controller (PLC)-based cabinets using a PLC for bus stripping and load logic and control. The signal path structure of the PLC uses dedicated input modules, control logic, and dedicated output modules.

LOOP Signal Only

On a LOOP in a given unit, both sequencers associated with that unit will respond accordingly to clear their associated buses, stripping all 4.16KV loads and specified 480V loads within one second after the LOOP signal is generated. The Emergency Diesel Generators (EDGs) [EK:dg] will start, and within 15 seconds the EDG output breakers [EK:bkr] close, then loads required for safe reactor shutdown are sequentially connected to the corresponding bus; the first load block output signal is generated 16.5 seconds after the onset of the LOOP.

LOCA Signal Only

If either unit experiences a LOCA, and preferred (offsite) power is available, bus stripping signals and EDG breaker closure permissive signals will not be initiated by the sequencers. Vital loads will be sequentially connected to the buses by the sequencers (including the opposite unit's HHSI pumps). If an EDG is already operating and parallelled to offsite power, and either unit experiences a LOCA, the EDG breaker will trip. The EDG will continue to run in a standby condition. On the LOCA unit, Engineered Safety Feature (ESF) equipment will be sequentially loaded onto the bus by the sequencer. Following a LOCA, if any given train experiences undervoltage, bus stripping, EDG breaker closure, and sequentially loading will be directed.

LOOP/LOCA

After a LOOP on both units, if one unit experiences a LOCA, the buses associated with the LOCA unit will be stripped and ESF loads will be loaded onto the bus. On the non-LOCA unit, both buses are stripped again, and reloaded with essential equipment; both HHSI pumps will also start.

Sequencer Testing

Each sequencer is provided with Manual test and Automatic Self-test capability. The test mode is determined by a three-position Test Selector switch. The three positions are AUTO (self-tests 15 steps or scenarios in the automatic test sequence), MAN (each test is manually initiated), and OFF (no test signals are generated). In the automatic test mode, the sequencer continuously tests the input cards, output cards, and output relay coils, and exercises the program logic. The sequencer is designed to abort the manual and automatic test modes in response to a valid input. The automatic self-test function is normally in operation, however it is not required to be in service for the sequencer to perform its safety function. The manual test, in addition to testing all the conditions covered by the automatic test, actuates the output relays. However, blocking relays energize before the output relays energize, and the output relays de-energize before the blocking relays de-energize.

Placing the Test Selector switch in MAN stops automatic self-testing.

Manual testing involves five stripping/clearing scenarios (bus clearing, 480V undervoltage with SI present, 480V degraded voltage, 4.16KV undervoltage, and safety injection [LOCA] on an isolated bus). Upon completion of the stripping tests, sequencing scenarios are tested manually by rotation of a Sequencing Mode Test Selector switch through eleven steps or loading scenarios (LOOP; LOOP/LOCA same train; LOOP/LOCA other unit; LOCA same train; LOCA other unit; LOOP/LOCA same train with concurrent HHCP; LOOP/LOCA same train with HHCP before 13 seconds; LOOP/LOCA same train with HHCP after 13 seconds; LOCA same train with concurrent HHCP; LOCA same train with HHCP before 13 seconds; LOCA same train with HHCP after 13 seconds).

Automatic self-testing cycles through 15 of the 16 test steps in the same order (the bus clearing scenario is not tested in AUTO). The test steps start roughly an hour apart, and there is one hour in the automatic test sequence in which no testing takes place, so a full cycle of automatic self-testing takes approximately sixteen hours. Then the cycle begins again. Should a valid process input signal be received during manual or automatic testing, the testing stops, the test signal clears, and the inhibit signal is supposed to clear if present, allowing the valid signal to sequentially energize the output relays and their associated ESF equipment.

II. CAUSE OF THE EVENT

The 3A sequencer failed to respond as expected to an opposite unit SI signal. 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 LED for a 4A SI 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 after a 3 second delay. However, the pump failed to start because it did not receive a start signal from the sequencer.

Following the failure of 3A HHSI pump to start in response to a 4A SI input signal as described above, an analysis of the sequencer software logic was performed to determine the root cause of the failure. A software design defect was discovered whereby the start signal for the 3A HHSI pump remained inhibited during sequencer automatic test step 3 (LOOP/LOCA other Unit) even though a valid process input was present. In parallel with the above analysis, this particular fault was duplicated on the sequencer simulator which is identical to the 3C23A-1 (3A) sequencer. This is in contrast to the original design bases of the sequencer Automatic Self-Test and Manual Test functions.

The review was then expanded to include additional test modes, process inputs, and required outputs. It was found that the problem exists during both manual and automatic testing, during sequencer test steps 2, 3, 6, 8, and 10. These steps correspond to the following scenarios:

Step 2	LOOP/LOCA
Step 3	LOOP/LOCA other Unit
Step 6	LOOP/LOCA with concurrent High High Containment Pressure
Step 8	LOOP/LOCA with High High Containment Pressure less than 13 seconds later
Step 10	LOOP/LOCA with High High Containment Pressure more than 13 seconds later

Note that these are tested scenarios, not potential plant events. Note too that all five of the affected test step scenarios involve LOOP and LOCA.

If a valid SI signal is received 15 seconds or later into one of the above tests, the test signal clears as intended, but the inhibit signal is maintained by means of latching logic. This latching logic is originally established by the test signal, but may be maintained by the process input signal if it arrives prior to removal of the test signal.

Since the above condition is applicable to both the automatic self-test and manual testing, the sequencer must be considered inoperable during both testing modes. Note, however, that this defect will not cause a sequencer operating malfunction with the Test Selector switch in any position for any design basis scenario which involves a loss of offsite power.

This software logic defect was introduced during the detailed logic design phase of the software development. The detailed logic designer and the independent verifier failed to recognize the interaction between some process logic inhibits and the test logic. The defect in the software logic was not detected during the Validation and Verification process (V&V) because the response to valid inputs was not tested during all stripping and loading sequences of the automatic and manual testing logic. FPL has evaluated the V&V for the sequencers and concluded that the existing V&V adequately addresses operation of the sequencers with the Test Selector switch in OFF.

This logic defect can occur when the sequencer is in either the manual or automatic test mode, and the test sequence currently being executed is loading sequence test 2, 3, 6, 8, or 10. This was determined based on a review of the sequencer logic drawings for the 15 steps in the automatic test sequence, and design basis event signals. The sequencer simulator was used to confirm the results of the review. The defect cannot affect sequencer operation with the Test Selector switch OFF.

In loading sequence tests 2, 6, 8, or 10, the sequencer may be inhibited from responding to a valid SI signal on the same train. In loading sequence test 3, the sequencer may be inhibited from responding to a valid SI signal on the opposite unit.

III. ANALYSIS OF THE EVENT

As a result of the erroneous inhibit signals, the potential exists for any sequencer output to be prevented from being generated when required. Exactly which output or outputs is(are) determined by a combination of factors, i.e., which test scenario is in progress, how long since the test scenario was initiated, and which process input or inputs are received. In general, for the approximate one-hour duration of each of the above test steps (with the Test Selector switch in AUTO), the sequencer will not respond correctly to a valid process input signal.

With the sequencer Test Selector switch in AUTO, the sequencer steps sequentially through sixteen steps as described above; first the five bus stripping/clearing steps, followed by the eleven LOOP and/or LOCA scenarios. Note that the five test steps affected by the software defect are all in the loading sequence test steps, so the first affected step is the seventh step in the total testing sequence. During each of these affected test steps, fifteen seconds after the initiation of the step, the sequencer would not have responded properly to a valid process input signal. So the sequencer was inoperable for about five hours out of each sixteen hour period as long as its Test Selector switch was in AUTO. The sequencer was also inoperable for the duration of any Manual test of the five test steps listed above. A complete manual test on one sequencer takes about one hour.

POTENTIAL ACCIDENT CONSEQUENCES FOR SEQUENCER FAILURE MODES

Test Logic Defect
The review of the sequencer logic determined that improper operation of the sequencer could occur for only certain sequencer stripping/loading scenarios in which an SI signal without LOOP occurs. The sequencer logic software defect does not affect any scenarios where a LOOP also occurs, whether before, after, or concurrent with an SI signal. A failure modes and effects matrix identified the following four potential plant events where the logic software defect could affect the operation of the sequencer, depending upon which of the five affected test steps (discussed above in II. CAUSE OF THE EVENT) are being performed when the SI signal is received by the sequencer:

#1 LOCA Same Train

#2 LOCA on other Unit

#3 LOCA w/High High Containment Pressure (HHCP) < 13 seconds

#4 LOCA w/HHCP > 13 seconds

Note that these are potential plant events, not test step scenarios. Note too that in contrast to the list of affected test step scenarios presented earlier, none of the potential plant events affected involve a LOOP.

For each of these events, the sequencer could receive a valid SI signal but the logic defect could inhibit the sequencer from starting equipment. Events #1, #3, and #4 above each have four logic test steps out of a total of sixteen which would inhibit the sequencer from providing a start signal to the equipment it controls while event #2 is affected by only one of the sixteen logic test steps.

The probability that an individual sequencer would not respond to a valid same train SI signal is 4 hours/16 hours = 2.5E-1. The probability that an individual sequencer would not respond to a valid opposite unit SI signal is 1 hour/16 hours = 6.25E-2.

The equipment affected due to the failure of a sequencer was identified from plant drawings. The equipment listed below is specific to the 3A sequencer. The equipment lists would be similar for the other three sequencers.

For event #1, the following equipment would not be automatically loaded by the sequencer:

Residual Heat Removal Pump 3A [BP:p]
HHSI Pump 3A
Intake Cooling Water Pumps 3A (1) and 3C (1) [BI:p]
Emergency Containment Cooler Fan 3B and 3C [BK:fan]
Component Cooling Water Pumps 3A (1) and 3C (1) [CC:p]
Emergency Containment Filter Fans 3B and 3C {BK:fan]

Note (1): The equipment identified may already be in operation and may not require manual action to start.

For events #3 and #4 (LOCA w/HHCP < 13 sec; LOCA w/HHCP > 13 sec), Containment Spray Pump 3A would be affected in addition to the equipment identified above for event #1.

For event #2 (LOCA other Unit), only the 3A HHSI Pump would not be automatically started.

It should be noted that one of the initiating signals for Auxiliary Feedwater (AFW) system [BA:p] is bus stripping, which is controlled by the sequencer. No credit is taken, however, for bus stripping in the accident analyses for initiating AFW. AFW is also initiated on low-low steam generator level, SI, manual initiation and trip of all Main Feedwater pumps [SJ:p].

Using the above information, the defect in the sequencer test logic represents a potential concern for events where SI is required for mitigation and no LOOP is experienced.

CS Pump Autostart Software Error
Using the Turkey Point baseline Probabilistic Safety Assessment model, the probability of dual train failure of the CS system if called on to operate has been estimated to be approximately 2.6E-3. This estimate reflects CS system and support system component failure probabilities not including either of the software errors reported here.

The failure to automatically start a CS pump due to this software error can only occur under a very remote set of circumstances. The 60 ms window is on the same order as the tolerance on relay pick-up times and the sequencer processing and timing tolerances. Even with sophisticated timing equipment, it is unlikely that the failure mode could be demonstrated repeatedly. The probability of receipt of a HHCP signal during a 60 ms window of vulnerability compared to the range of timing conditions for which the sequencer is designed is considerably smaller than the overall system reliability identified above. If it is assumed that HHCP can occur at any time within approximately two minutes after the SI signal (the earliest time at which SI is postulated to be reset), then the probability of the evaluated condition occurring on one train is:

$$0.060 \text{ sec}/(2 \text{ min} \times 60 \text{ sec/min}) = 5.0\text{E-}4$$

The estimate of the probability of a CS pump not starting automatically in a LOCA or LOOP/LOCA due to the reported software error is therefore approximately a factor of five below the estimated probability of both CS trains failing during a design basis event.

The probability of the software error affecting both trains is considerably lower, since it would require: 1) the initiating SI signals to be at the sequencer inputs within 60 ms of each other; 2) the two trains of HHCP both occurring within the 60 ms window of vulnerability; 3) the sequencer input processing times to be identical; and 4) the timing of the two sequencers in synchronization. The difference in the cumulative delay time for relay actuations on the two trains of ESFAS and differences in sequencer processing, in all likelihood would be sufficient to preclude the condition on both trains. This conclusion is supported by a review of previous Integrated Safeguards Test data. The difference between the train A and B CS pump recorded start times during a simulated LOOP/LOCA has been between 90 and 500 ms. Since some timing differences between the trains can be expected, and timing differences greater than 60 ms have been recorded during previous safeguards tests, the probability that the specific error could affect both trains of Containment Spray is therefore considerably less than the single train probability.

Effect on Analyzed Accidents

A review of the Turkey Point UFSAR Chapter 14 Accident Analyses was performed to determine which accidents would be potentially affected by the sequencer test software logic defect. This review identified 7 of the 22 accidents which may be affected. Two of the seven, "Loss of External Load" and "Loss of A.C. Power" were determined to be dependent on the sequencer but not affected, since the inhibited sequencer failure mode applies to loss of coolant accident (LOCA) scenarios only, i.e., no LOOP.

The five accidents both requiring SI, and affected by the sequencer test software logic defect, are the following:

1. Large Break Loss-of-Coolant Accident (LBLOCA)
2. Small Break LOCA (SBLOCA)
3. Rupture of a Steam Pipe (Main Steam Line Break, or MSLB)
4. Steam Generator Tube Rupture (SGTR)
5. Rupture of a Control Rod Mechanism Housing

The effects of the sequencer test logic defect will be discussed below for each of the five accidents. In each case, the transient is described and equipment necessary for mitigation of accidents is identified. Each transient is then evaluated assuming all four sequencers fail to operate properly. Credit is assumed for operator action to start HHSI pumps as well as other ESF equipment within 10 minutes as described below.

LARGE BREAK LOSS OF COOLANT ACCIDENT

A LOCA would result from a rupture of the Reactor Coolant System (RCS) or any line connected to that system up to the first closed valve. For a postulated LBLOCA, a reactor trip is initiated by pressurizer low pressure (1790 psig) while the SI signal is actuated by pressurizer low pressure at 1636 psig. The consequences of the LBLOCA are limited in two ways:

1. Reactor trip and borated water injection supplement void formation in causing rapid reduction of nuclear power to a residual level corresponding to fission product decay.

2. Injection of borated water ensures sufficient flooding of the core to prevent excessive temperatures and provide long term cooling.

The reactor is designed to withstand the thermal effects caused by a LBLOCA including the double ended severance of the largest RCS pipe. The reactor core and internals, together with the Emergency Core Cooling System (ECCS), are designed so that the reactor can be safely shutdown and the essential heat transfer geometry of the core will be preserved following an accident.

The LBLOCA analysis presented in Section 14.3 of the UFSAR assumes that 2 of 4 HHSI pumps and 1 of 2 RHR pumps are automatically actuated during the accident. If all four sequencers were inoperable because of the simultaneous presence of the test logic defect, SI actuation would not occur automatically.

The LBLOCA is a design basis event whose probability of occurrence is extremely small. A LBLOCA is considered to be a break with a total cross-sectional area equal or greater than 1.0 ft^2.

LBLOCA sensitivity studies, performed in 1988 to assess the impact of delaying SI, indicate that the maximum permissible SI delay is about 1 minute in order not to exceed the Peak Clad Temperature criteria of 10 CFR 50.46, and about 5 minutes to avoid exceeding fuel melt temperature, for a generic Westinghouse four-loop PWR. As a result of the test logic defect, Turkey Point tested operator reaction times to manually start SI in the absence of an automatic start (described below under **MITIGATION OF SEQUENCER FAILURE MODES**). The maximum time did not exceed 4 minutes. This information was provided to Westinghouse, who then determined that if SI is delayed 3 minutes and 15 seconds, the peak clad temperature for the hot rod will not exceed 1922 degrees Fahrenheit. If a conservative adiabatic heat up rate of six degrees per second is assumed for the fuel, SI may be delayed until four minutes into the LOCA without exceeding 10 CFR 50.46 PCT criteria. Therefore,if reasonable operator action is credited, no core damage would be expected.

Containment Response to a LBLOCA

A LBLOCA results in a significant mass and energy release into containment that results in pressurization of the containment structure. The UFSAR indicates that the pressurization event is limited by the size of containment, by containment heat sinks, and by the operation of containment cooling equipment (containment sprays and emergency containment coolers).

The containment analysis for the LBLOCA was assessed using better estimate techniques in 1989 by Westinghouse. This analysis showed that peak containment pressure for a Double Ended Pump Suction (DEPS) to be on the order of 42 to 45 psig. Using the mass and energy release values developed for the design basis reconstitution work, Westinghouse re-performed the Turkey Point containment analysis assuming no operation of the containment spray pumps or the emergency containment coolers, for ten minutes. This reanalysis shows that the peak pressure of the DEPS LOCA to be approximately 44.3 psig. Accordingly, since this peak pressure is less than the design pressure of 55 psig and less than the originally analyzed peak pressure of 49.9 psig, the results are acceptable. The ultimate strength of the Turkey Point containments is estimated to be approximately 140 psig based on the Individual Plant Examination (IPE) analysis work.

Dose Consequences for a LBLOCA

The UFSAR contains an offsite dose evaluation that assumes a total core release (100% noble gas, 50% halogens) occurring at time t = 0 with results that remain within 10 CFR Part 100 guidelines. The event under review, however, is different than that evaluated in the UFSAR in that engineered safety features are assumed to be delayed. Using knowledge learned from observation of accident phenomena and advanced light water reactor development programs, it has been concluded that an instantaneous core melt and release of fission products to containment is not credible. Rather, significant release to the containment would not be expected to occur during the first ten minutes of an accident. During this time, credit is taken for operator action to start SI, containment sprays, etc. Manual actuation of the containment sprays and emergency filters would provide for fission product cleanup within containment. While a calculation has not been performed, it is expected that the offsite dose consequences for this event will not exceed those stated in the UFSAR. Operation of sprays and filters will provide radioactive material cleanup prior to any significant fission product release from the containment.

SMALL BREAK LOSS OF COOLANT ACCIDENT (SBLOCA)

SBLOCAs are slow transients which take longer to initiate SI and therefore are less sensitive to delays in the actuation of the HHSI pumps. Containment response and dose consequences for the SBLOCA event are bounded by LBLOCA discussions above.

MAIN STEAM LINE BREAK

The UFSAR analyzes two separate steam line break events; opening a relief or safety valve, and main steam piping failure. The piping failure bounds the opening of the relief or safety valve. Since the sequencer issue is only a concern for the offsite power available case, only a main steam piping failure with offsite power available will be addressed. The most limiting cooldown event occurs at zero power with no decay heat. As indicated in the UFSAR, credit is taken for a single HHSI pump to provide borated water to return the core to a subcritical state.

Westinghouse re-performed the limiting MSLB accident with offsite power available assuming SI was not available for ten minutes. The results of this analysis indicate that the event can be accommodated without SI for ten minutes with acceptable results.

Containment Response to an MSLB

A Main Steam Line Break inside containment also results in a containment pressurization transient. This event was rerun by Westinghouse assuming no active containment pressure mitigating features (i.e. no containment sprays or containment coolers). Assuming no safeguards actuation, peak containment pressure for the MSLB was 48.8 psig occurring approximately 300 seconds (5 minutes) into the transient. This is within the containment design pressure of 55 psig and is therefore acceptable.

STEAM GENERATOR TUBE RUPTURE

The event examined in the UFSAR is a complete tube break adjacent to the tube sheet. Each steam generator tube has a nominal diameter of 0.875 inches with a wall thickness of 0.050 inches. Accordingly, the cross-sectional break area of a double ended tube rupture is less than 1.0 square inches. This small break area shows that this event is bounded by the SBLOCA in terms of assessing the potential for core damage resulting from this event, and that dose releases for this event will not increase as a result of delayed SI.

RCCA EJECTION - RUPTURE OF A CONTROL ROD MECHANISM HOUSING

The event examined in the UFSAR is a failure of a control rod mechanism pressure housing such that RCS pressure would eject the control rod and drive shaft to a fully withdrawn position. The consequence of this mechanical failure is a rapid positive reactivity insertion together with an adverse core power distribution. The reactivity transient is terminated by the Doppler reactivity effects of the increased fuel temperature, and by subsequent reactor trip before conditions are reached that can result in fuel melt.

Actions are included in the Emergency Operating Procedures (EOPs) to address a SBLOCA that could be caused by a failed control rod mechanism pressure housing. Accident consequences of a SBLOCA in the reactor vessel upper head are bounded by the design-basis SBLOCA in the cold leg.

Summary of Potential Accident Consequences

Of the five UFSAR accidents affected, four are bounded by the LBLOCA. Consequences of a LBLOCA are acceptable if operator action to start ESF equipment takes place within four minutes of the start of the accident. The consequences of a MSLB are acceptable without operator action for ten minutes, since containment pressure peaks, below the design pressure, five minutes into the accident.

MITIGATION OF SEQUENCER FAILURE MODES

Because the presence of an SI signal during sequencer testing (automatic or manual mode) may render the sequencer inoperative, the dependence on SI was the primary consideration for determining the five affected accidents. For each of the affected accidents, the EOPs were reviewed to determine what mitigating actions would be taken by the operator. The effectiveness of the mitigating actions was also assessed based on its sequence within the procedures.

Upon initiation of any of the five affected accidents discussed above, the reactor would trip placing the operators in procedure 3/4-EOP-E-0, "Reactor Trip or Safety Injection." At Step 4 in EOP-E-0, the operator verifies whether SI is actuated or is required. If an SI is required, the operator verifies that HHSI and RHR pumps have started, or he is required to manually start these pumps in Step 8. These two steps are part of the immediate actions to be taken by an operator following a reactor trip.

In addition, the foldout pages for EOP-E-0 contains specific reactor trip and SI actuation criteria which require operators to start the HHSI pumps. Therefore FPL concludes that for these five accidents, there is a high probability that timely mitigating actions would have been taken by the operators to activate safeguards equipment even if the sequencer had failed.

To assess the operators' ability to accommodate sequencer test software logic defects, the Turkey Point Training Department constructed three different scenarios involving design basis accidents with failed sequencers. The failure mode modeled was a failure of the sequencer to load safeguards equipment. These scenario runs were completed on November 5, 1994. The three scenarios were:

1. A LOOP/LBLOCA with Unit 3 sequencers failed.

2. A LBLOCA with no LOOP, with Unit 3 sequencers failed.

3. A SBLOCA with no LOOP, with Unit 3 sequencers failed, Unit 4 HHSI pump breakers racked out, and the Unit 3 HHSI pump control switches in PULL TO LOCK on the Unit 4 control board.

Six control room crews ran each of the three scenarios, for a total of 18 simulator exercises. The Training Department was primarily interested in determining how long it took the control room crew to successfully energize all available safeguards equipment. A summary of the control room crew response times follows:

CREW	RESPONSE TIMES FOR FULL SAFEGUARDS INITIATION (IN MIN:SEC)		
	LOOP/LOCA SCENARIO	LBLOCA SCENARIO	SBLOCA SCENARIO
A	2:40	2:30	2:45
B	2:00	2:10	1:40
C	2:50	1:30	1:30
D	8:00	1:30	1:55
E	4:40	3:15	1:05
F	2:50	1:32	1:20

The simulator training coordinator stated that the longest time required to initiate SI flow was during Crew D's 8 minute LOOP/LOCA scenario; it took them approximately 4 minutes. However, the sequencer defect is not present for LOOP scenarios. The longest non-LOOP response time was 3 minutes and 15 seconds. An assumed operator response time of 10 minutes is therefore conservative.

In addition to the scenario exercises described above, a review of earlier observations of operating crews in simulator training during July and August 1994 was made. These observations illustrated that it took each crew 4 to 5 minutes from event initiation to complete alignment of the required safeguards equipment associated with a full sequencer failure.

Operator verification of SI, and HHSI pump flow, is performed within the immediate action steps (Steps 4 and 8 respectively) of EOP-E-0. The first 14 steps are memorized by the control room crew. In addition, immediate action steps are required to be re-verified by the operators. Therefore FPL concludes that the control room crew would be successful in timely initiation of HHSI pump flow in the event of a sequencer malfunction.

PROBABILISTIC SAFETY ASSESSMENTS

A probabilistic safety assessment was performed to estimate the safety impact of inhibited emergency sequencer operation due to a logic error in the software associated with the test feature. The assessment is based on the Turkey Point IPE Submittal and subsequent updates, and includes the effect of the failure of all four sequencers. The recovery actions are added to the model for different scenarios, e.g., recovery for LBLOCA vs. SBLOCA. These operator actions are calculated based on the time available to do the actions (NUREG/CR-4550, Vol. 3, Rev. 1, Part1), and the time it takes the operators to perform the actions obtained from a review of 3/4-EOPs-0 and from simulator scenario runs.

The probabalistic safety assessment determined that the estimated change in the Core Damage Frequency (CDF) under the above conditions, with all four sequencers inoperable, is 6.3E-6/yr. However, all four sequencers were not inoperable at all times. Each sequencer is inoperable during 5 of the 16 tests. In order for all sequencers to fail simultaneously, all sequencers would have to be in an affected test. This would happen most often if all four sequencer test cycles were synchronized. Even if all four sequencers were synchronized on the same test cycle, the sequencers would all be inoperable during only 5 of the 16 tests. Therefore, all four sequencers would be inoperable approximately one-third of the time. This results in an estimated change in CDF of 2.1E-6/yr. This change in core damage frequency increases the baseline CDF by 3.2%. The PRA calculation considers an average probability over a one year period.

The 3.2% increase in the CDF is a conservative estimate for this situation. This increase in CDF is not safety significant, based on the acceptance criteria stipulated in the draft EPRI PSA Application Guide.

The estimated risk impact of loss of sequencers for LBLOCAs is relatively low due to the low initiating event frequency of LBLOCAs, and recovery actions described in the early steps of the EOP E-0 for reactor trip and SI. Although SBLOCAs have a higher initiating event frequency the risk is relatively low because the operator has more time available to perform recovery actions.

An estimate of the potential risk impact of the failure of the CS pumps to automatically start was performed. The scenario is assumed to occur for a certain size LOCA or MSLB such that the HHCP signal is generated at the 12.9 to 13.0 second window during which the sequencers may not actuate CS pumps automatically. A further assumption is that failure of all containment spray with a medium LOCA leads directly to core damage. The core damage frequency increase is thus estimated to be:

CDF = (frequency of event [medium and small LOCAs, MSLB]) times
(probability of "right size" break to cause the event) times
(probability of failure of manual starting of CS pumps)

= (1.0E-4 + 1.0E-3 + 1.0E-4) x (5.0E-4) x (6.0E-3)

= 3.6 E-9 / year

Note that the frequency of the event is conservatively estimated to be that of the medium LOCA (6-13.5 inches), the small LOCA (2-6 inches) or a MSLB. Since a specifically-timed LOOP would be required for either the small LOCA or the MSLB to be of concern, the CDF is actually lower.

A estimated increase in the CDF of 3.6E-9/yr is insignificant compared to the baseline CDF of 6.63E-5/yr.

SAFETY SIGNIFICANCE AND OPERABILITY

The periodic inoperability of all four sequencers, as described above, has existed since the sequencers were installed during the dual unit outage in 1990/1991. The sequencers were accepted as operational in September and October, 1991, for Units 3 and 4, respectively. From early December, 1991, until November, 1992 (Unit 3) and May, 1993 (Unit 4) the sequencers' Test Selector switches were in OFF except for monthly manual tests, as described in LER 251/91-007.

Since then, there have been four challenges to the bus sequencers (between the two units). LER 251/92-004 reported an inadvertent Safety Injection on Unit 4; all plant equipment responded as designed, including the Unit 3 HHSI pumps. LERs 250/92-009 and 250/92-013 reported a LOOP (due to hurricane Andrew), and an inadvertent 3A bus stripping. In these three instances the sequencers' Test Selector switches were not in AUTO, and they performed as designed.

LER 250/94-002 reported an inadvertent ESF actuation on Unit 3, in which all equipment responded as design, except the 4A HHSI pump. At that time the failure of the 4A HHSI pump was attributed to an intermittent failure, which could not be reproduced. As a result of the discovery of the defect reported herein, that earlier event can now be reproduced at will on the sequencer simulator. FPL believes that the 4A HHSI pump failed to start because of the same defect that caused the 3A HHSI pump failure to start, reported in this LER.

Since there have been no actual events requiring Engineered Safety Features actuation to protect the plant, the health and safety of the public has not been affected by the periodic inoperability of the sequencers.

This event is reportable under the requirements of 10 CFR 50.73(a)(2)(i)(B), (a)(ii)(A), (a)(ii)(B), (a)(v), (a)(vii), and 10 CFR 21.

Regarding the second software error involving the CS pump autostart, FPL has concluded that the CS system remains OPERABLE because, in the highly unlikely event that the condition were to occur, simple operator action to start the CS pumps, in accordance with the plant's emergency operating procedures, would ensure compliance with the system specified functions. The ability to manually start the CS pumps as much as ten minutes into the event and maintain required cooling is supported by analysis, procedures, and training. In addition the safety significance of the evaluated condition is extremely low because the probability of the evaluated condition is lower than the probability of a common mode failure of both CS trains, as discussed earlier under Possible Accident Consequences for Sequencer Failure Modes. In any case, the contribution to CDF of this software error is negligible.

IV. CORRECTIVE ACTIONS

1. The Test Selector switches on all four sequencers were placed in OFF. Tags have been hung on each switch to require specific permission from the Nuclear Plant Supervisor to change the position of the switch. With the sequencer test mode switch in the OFF position, the automatic test logic is disabled. The sequencer is fully functional and will respond properly to input signals. The automatic test function is not a requirement for periodic surveillance of the sequencer.

2. With the Test Selector switch in OFF, additional visual inspections are being performed on a eight hour basis as described below:

   a. The local reflash annunciators points are verified not in alarm.

   b. The I/O power, PLC Power, and ANN Power switches are verified in the ON position and the Processor Power white indicating light is verified illuminated.

   c. The Test Selector switch is verified in the OFF position; the Stripping Clearing Test Selector and Sequencing Mode Test Selector Switches are verified in the OFF position.

   d. The 2 green test reset indicating lights and the sequencing reset green indicating lights are verified illuminated.

   e. The other indicating lights are verified not to be illuminated (except the ground fault indicating lights are supposed to be dimly lit).

   f. Every 24 hours, the sequencer door is opened, the Processor Indicator LED is verified to be a solid green and the 9 indicator I/O cards "ACTIVE" LED are verified to be a solid green.

3. A detailed review of the original Validation and Verification process was performed; it has been concluded that an oversight occurred because not all sequencer functions were validated during all modes of automatic and manual testing. The existing verification and validation sufficiently covers the sequencer safety functions if the Test Selector switch remains OFF.

4. Functional testing on the sequencer simulator of design basis inputs has been repeated with the Test Selector switch OFF, with acceptable results.

5. A safety evaluation has been issued demonstrating sequencer operability with the test selector switch in the OFF position. This safety evaluation was approved by the Plant Nuclear Safety Committee on November 4, 1994.

6. Independent consultants were retained to perform an assessment of the existing sequencer design, software design and V&V. This "Independent Assessment Team" (IAT) concluded that operation of the sequencers with the Test Selector switch in OFF represented a safe condition and that FPL's evaluation of the condition was appropriate.

   The second phase of the IAT's assignment was to provide a detailed review of the software documentation. Some drawing discrepancies were identified and have been evaluated. In general the discrepancies dealt with the inclusion of additional information on the logic diagrams not reflected in the ladder diagrams, to aid in understanding the logic diagrams. One other software error was identified involving autostart of the CS pumps, and has been discussed earlier in the LER. The drawing discrepancies will be corrected when the software is modified (see Corrective Action #9 below).

   The IAT confirmed that the V&V was not comprehensive enough to test certain aspects of the logic. "The plan was weak in that it relied almost completely on testing as the V&V methodology. More emphasis on the analysis of the requirements and design would have increased the likelihood of discovering the design flaw." A revision to the V&V documentation will be made coincident with the design modifications described on Corrective Action #9 below.

7. The original software vendor, United Controls, Inc. has been notified of this defect and its significance.

8. In order to eliminate issues related to the use of one-of-a-kind or first-of-a-kind equipment, FPL implemented Nuclear Policy NP-905, Equipment Selection, in October of 1991. This policy states in part that, "FPL's nuclear engineering department shall select only specific models of equipment with proven records of reliable performance for use in FPL nuclear facilities. Verification of the equipment reliability must be established through contact with NPRDS, nuclear station managers, or other appropriate sources. If no prior operating experience is available, appropriate prototype testing, under equivalent plant operating conditions, must be undertaken to establish its reliability before it is placed in service at FPL nuclear facilities." The Engineering Quality Instructions contain the Nuclear Policy requirements for design outputs.

9. Design modifications to eliminate the software logic problems will be implemented during the next refueling outages of each unit.

10. Other safety-related process computer suppliers were notified of the event on November 14, 1994. These suppliers responded that similar software errors do not exist in other safety-related process computers.

11. An FPL Nuclear Engineering standard will be developed on the use of PLCs, prior to the procurement of any additional PLC-based equipment.

12. Manual testing of the sequencers was resumed on January 11, 1995.

V. ADDITIONAL INFORMATION

EIIS Codes are shown in the format [EIIS SYSTEM: IEEE component function identifier, second component function identifier (if appropriate)].

The Programmable Logic Controllers used in the sequencers are made by Allen-Bradley; the sequencers are assembled by United Controls, Inc. (UCI). According to UCI, Florida Power & Light Company is the only utility to which UCI supplied this sequencer.