NRC Form 366
(9-83)

U.S. NUCLEAR REGULATORY COMMISSION
APPROVED OMB NO. 3150-0104
EXPIRES: 8/31/85

LICENSEE EVENT REPORT (LER)

FACILITY NAME (1)	DOCKET NUMBER (2)	PAGE (3)
Palisades Plant	0 5 0 0 0 2 5 5	1 OF 0 8

TITLE (4) MALFUNCTION OF THE LEFT CHANNEL DBA SEQUENCER RESULTS IN INADVERTENT ACTUATION OF LEFT CHANNEL SAFEGUARDS EQUIPMENT

EVENT DATE (5)			LER NUMBER (6)			REPORT DATE (6)			OTHER FACILITIES INVOLVED (8)	
MONTH	DAY	YEAR	YEAR	SEQUENTIAL NUMBER	REVISION NUMBER	MONTH	DAY	YEAR	FACILITY NAMES	DOCKET NUMBER(S)
									N/A	0 5 0 0 0
0 3	0 2	9 5	9 5	– 0 0 1 –	0 0				N/A	0 5 0 0 0

OPERATING MODE (9)	N
POWER LEVEL (10)	1 0 0

THIS REPORT IS SUBMITTED PURSUANT TO THE REQUIREMENTS OF 10 CFR §: *(Check one or more of the following)* (11)

□ 20.402(b)	□ 20.405(c)	☒ 50.73(a)(2)(iv)	□ 73.71(b)
□ 20.405(a)(1)(i)	□ 50.36(c)(1)	□ 50.73(a)(2)(v)	□ 73.71(c)
□ 20.405(a)(1)(ii)	□ 50.36(c)(2)	□ 50.73(a)(2)(vii)	□ OTHER (Specify in Abstract below and in Text, NRC Form 366A)
□ 20.405(a)(1)(iii)	□ 50.73(a)(2)(i)	□ 50.73(a)(2)(viii)(A)	
□ 20.405(a)(1)(iv)	□ 50.73(a)(2)(ii)	□ 50.73(a)(2)(viii)(B)	
□ 20.405(a)(1)(v)	□ 50.73(a)(2)(iii)	□ 50.73(a)(2)(x)	

LICENSEE CONTACT FOR THIS LER (12)

NAME	TELEPHONE NUMBER
	AREA CODE
William L. Roberts	6 1 6 7 6 4 - 8 9 1 3

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

CAUSE	SYSTEM	COMPONENT	MANUFAC-TURER	REPORTABLE TO NPRDS	CAUSE	SYSTEM	COMPONENT	MANUFAC-TURER	REPORTABLE TO NPRDS

SUPPLEMENTAL REPORT EXPECTED (14)		EXPECTED SUBMISSION DATE (15)	MONTH	DAY	YEAR
☒ YES *(If yes, complete EXPECTED SUBMISSION DATE)*	□ NO		1 0	0 1	9 5

ABSTRACT *(Limit to 1400 spaces, i.e., approximately fifteen single-space typewritten lines)* (16)

On March 2, 1995, at 2009 hrs, with the plant operating at 100% power, the left channel Design Basis Accident (DBA) sequencer malfunctioned and simultaneously started most of the left channel safeguards equipment. Some left channel safeguards equipment was blocked from starting by logic external to the sequencer. All safeguards equipment responded as required and the plant response was normal for the equipment that changed status. Plant power was reduced to 91% because of the event. The safeguards equipment was secured and the left channel sequencer and corresponding diesel generator declared inoperable.

Instrument and Control personnel documented the as-found condition of the sequencer. Testing was performed in the I&C lab to diagnose sequencer components. A team was established to determine root cause, evaluate common mode failures, and make recommendations to management regarding the sequencer. Evaluation determined that a failure of the micro-processor module of the electronic DBA sequencer caused the event. The micro-processor was replaced, operability of the sequencer verified and the plant returned to 100% power on March 4, 1995.

LICENSEE EVENT REPORT (LER) TEXT CONTINUATION

FACILITY NAME (1)	DOCKET NUMBER (2)	LER NUMBER (3)			PAGE (4)
		YEAR	SEQUENTIAL NUMBER	REVISION NUMBER	
Palisades Plant	0 5 0 0 0 2 5 5	9 5	– 0 0 1 –	0 0	0 2 OF 0 8

Event Description

On March 2, 1995, at 2009 hrs, the left channel DBA sequencer, MC-34L, malfunctioned and simultaneously started the left channel High Pressure Safety Injection (HPSI) pump (P-66B), Low Pressure Safety Injection (LPSI) pump (P-67B), boric acid pump (P-56B), service water pump (P-7B), closed the volume control tank outlet valve (MO-2087), opened the boric acid gravity feed valves (MO-2169, MO-2170), opened the LPSI loop isolation valves (MO-3008, MO-3010), and opened the HPSI loop isolation valves (MO-3007, MO-3009, MO-3011, and MO-3013). Charging pump (P-55C) started and was immediately stopped by pressurizer level control logic. Absent, as expected, from equipment actuation were the left channel auxiliary feedwater pump, (P-8A) and the left channel control room ventilation fan (V-95). Control room operators noted no precursor to this failure and also noted that it appeared that all sequencer actuations occurred simultaneously. During this event at least two of the safety injection tank pressure control valves (CV-3042, CV-3046, CV-3047 and CV-3038) opened causing relief valve RV-3161 to lift and relieve to the quench tank (T-73).

Plant power response was normal for the equipment that changed status during this event. The addition of boric acid caused reactor T_{ave} to decrease. The operators reduced power to 97% to match T_{ave} to T_{ref}. The operating charging pump (P-55A) automatically tripped on low suction pressure because the Volume Control Tank (VCT) outlet valve (MO-2087) closed as expected. The operators then isolated letdown. This left concentrated boric acid in the charging system. As a pre-planned evolution, charging and letdown were reestablished. This resulted in the power plant stabilizing at 91% power.

All safeguards equipment was secured, the left channel sequencer and associated diesel generator declared inoperable and a seven day limiting condition of operation for the diesel generator was entered. The right channel diesel generator was test started and off-site power verified. Instrument and Control (I&C) technicians and engineers were called in to evaluate and support the follow-up to the event.

The sequencer is a Programmable Logic Controller (PLC) that consists of a main micro-processor and various input/output (I/O) modules for each piece of equipment actuated by the sequencer. The as-found status of the sequencer indicated that a problem had occurred with the micro-processor module. The micro-processor was taken to the I&C lab where evaluation determined that the micro-processor was now working properly. Next all of the I/O modules were taken to the lab where it was determined that they were also functioning properly. A spare micro-processor was obtained from stock and satisfactorily functionally tested with the sequencer I/O modules. On March 3, 1995 at approximately 0300 hrs the spare micro-processor and the existing I/O modules were installed in the left channel DBA sequencer chassis. Return of the sequencer to service was delayed pending plant management review of the event and the corrective actions taken.

On the morning of March 3, 1995, an engineering and management team was established to review the event. A call was made to the manufacturers technical service department which confirmed that the as found status of the micro-processor indicated that a failure of the micro-processor had occurred. The discussion with the technical service department also confirmed the plant conclusion that based on the as found status and testing of the I/O modules they were operable. At approximately 1500 hrs a plant management meeting was held to review the event. Based on the results of the review a decision was made to return the sequencer to service and schedule a sequencer operability test. At approximately 1900 hrs the sequencer was successfully returned to service. The left channel of Technical Specification Surveillance QO-1, "Safety Injection" was completed as a test of the sequencer's operability. After successful completion of the testing the sequencer and associated diesel generator were declared operable. The plant was returned to 100% power on March 4, 1995.

Cause of the Event

The cause of the event is the failure of the DBA sequencer micro-processor module. The root cause of the micro-processor module failure is unknown at this time and evaluation of the exact cause of the unit failure is being pursued with the manufacturer.

Analysis of the Event

The DBA sequencer, MC-34L (left channel) and MC-34R (right channel), sequence loads onto the emergency diesel generators. Sequencing of loads ensures that appropriate equipment is energized in time to contend with an event while at the same time preventing excessive step loads from being placed on the diesel generator (which could result in the loss of the generator).

Automatic sequencer actuation occurs only when emergency generator power is automatically demanded as result of lost or unacceptably degraded 2400V AC bus voltage. When this emergency generator demand is not accompanied by a Safety Injection Signal (SIS) actuation, the Normal Shutdown Sequencer (NSD) sequence is selected. When the emergency generator demand is accompanied by a SIS, the Design Basis Actuation (DBA) sequence is selected.

Issues/Questions

- **What did the sequencer do to cause the safeguards initiation?**

  Discussion with operations personnel and examination of Plant Datalogger Sequence of Events Report indicates that every sequencer output device was sent a "start" signal. Some devices were blocked from starting by logic external to the sequencer and as such were not reported on the datalogger report.

NRC Form 366A
(9-83)

U.S. NUCLEAR REGULATORY COMMISSION
APPROVED OMB NO. 3150-0104
EXPIRES: 8/31/86

LICENSEE EVENT REPORT (LER) TEXT CONTINUATION

FACILITY NAME (1)	DOCKET NUMBER (2)	LER NUMBER (3)					PAGE (4)
		YEAR		SEQUENTIAL NUMBER		REVISION NUMBER	
Palisades Plant	0 5 0 0 0 2 5 5	9 5	–	0 0 1	–	0 0	0 4 OF 0 8

At some time after initiating every output, the micro-processor turned off every output. Although it is difficult to determine exactly how long this took, it had to be long enough for equipment breakers and interposing relays to latch. The following are considerations in determining that time.

The sequencer can process its entire ladder logic program in 10 to 20 milliseconds. If the micro-processor "locked up" or if the processor diagnostic shut it down, it would take 300 milliseconds for the I/O cards to realize that communication with the micro-processor is absent or garbled. This is commonly referred to as a "watchdog" feature. The I/O card would then automatically turn off every output and extinguish its ACTIVE light. The as-found status lights indicate that the processor was either "locked up" or shutdown by diagnostics because all I/O module ACTIVE lights were extinguished and 300 milliseconds is long enough for the equipment breakers and interposing relays to latch.

- **What caused the sequencer failure?**

Although the final root cause is unknown, we believe we have eliminated every component as the cause except the sequencer's micro-processor unit. The following is support for this position.

The DBA sequencer chassis holds all of the sequencer I/O modules and is a passive device. Because the processor and I/O modules communicate across the chassis backplane using Cyclic Redundancy Checksum (CRC-16), which is a method for detecting communications errors within the sequencer, a fault on the backplane could not force the I/O module to alter the state of its outputs.

The I/O modules should not be able to make the processor fail its diagnostics because the error checking program (CRC-16) would not allow a fault on a single I/O card to be propagated to all output cards. A failure on the input card, however, could possibly start a false initiation of a NSD or DBD sequence which would take about 55 seconds to complete as determined by the software ladder logic. Since for this event, the sequencer actuated all outputs at once, this eliminates the input card as the source of failure.

Investigation of the "as found" sequencer condition showed that the micro-processor had the POWER light on, and the RUN and READY lights extinguished. The READY being off can only occur if the micro-processor locks up or the diagnostics detect a CPU or memory error and shuts down the system. The RUN and READY light on the micro-processor and the ACTIVE light on each I/O module were found off which is consistent with this failure mode. The Run light indicates that the processor is executing the ladder logic. If the micro-processor has been shutdown, it could not run logic programming.

NRC Form 366A
(9-83)

U.S. NUCLEAR REGULATORY COMMISSION
APPROVED OMB NO. 3150-0104
EXPIRES: 8/31/85

LICENSEE EVENT REPORT (LER) TEXT CONTINUATION

FACILITY NAME (1)	DOCKET NUMBER (2)	LER NUMBER (3) YEAR		SEQUENTIAL NUMBER		REVISION NUMBER	PAGE (4)
Palisades Plant	0 5 0 0 0 2 5 5	9 5	—	0 0 1	—	0 0	0 5 OF 0 8

The ACTIVE light on the I/O modules would automatically turn off if the processor failed due to a communication timeout. Therefore, we believe that the micro-processor was the only possible point of failure in the sequencer.

The following is speculation as to why the root cause failure is considered to be the micro-processor. It is based on general computer experience and very little hard evidence and may end up being discounted as further investigation takes place.

A faulty component can cause intermittent memory or processor error which will cause computer systems to appear to lockup or quit instantaneously. However, the computer often will perform many instructions, some correctly and some incorrectly, before locking up or the error being detected by continuous diagnostics. The Palisades DBA sequencer system operates in the following cyclic sequence: inputs retrieved, ladder logic performed, output sent, diagnostics run. This processing sequence would allow for some error to propagate from the memory and micro-processor to the output cards before detection by the diagnostics routine. This error might also remain in place until more problems lock up the processor or diagnostics shut down the system. Even an error which is present for only one scan cycle would leave outputs energized for 300 milliseconds until the watchdog timer on the I/O cards turned the outputs off. This could explain how a micro-processor problem could have been processed to the output cards resulting in a start of the left channel safeguards equipment.

- **Is this a recurring event?**

There are some similarities between the current sequencer failure and the single previous failure on record. This previous failure occurred 7/29/89 to the right channel sequencer (MC-34R). The similarity is limited to the loss of ACTIVE lights on the I/O cards and the inability to recreate the failure during troubleshooting. The previous failure, however, did not activate any outputs. The differences in failure modes and the time between failures are large enough that a short term concern of a recurring event is not warranted. This previous failure will be discussed with the vendor in conjunction with the evaluation of the current sequencer failure.

- **Is there a common mode failure that could affect the microprocessor replacement unit or the other channel?**

This topic was discussed with the manufacture's technical service department. They searched their service bulletins for similar symptoms and none were found.

LICENSEE EVENT REPORT (LER) TEXT CONTINUATION

FACILITY NAME (1)	DOCKET NUMBER (2)	LER NUMBER (3)					PAGE (4)
		YEAR		SEQUENTIAL NUMBER		REVISION NUMBER	
Palisades Plant	0 5 0 0 0 2 5 5	9 5	–	0 0 1	–	0 0	0 6 OF 0 8

A theory was proposed that electro-magnetic interference (EMI) from some other device near to the micro-processor could have caused the problem. The theory was tested in the lab by keying a portable radio transmitter within a couple of inches of the micro-processor and monitoring for lockup or status light changes. None were detected. Power and input signals were examined for signal strength and wave form and nothing unusual was found. It has also been determined that no person was in close proximity to the sequencer when event occurred. At this time there appears to be no external mechanism to explain this malfunction of the micro-processor.

A typical consideration when software is involved with equipment operation is whether a certain combination of internal software logic and/or external inputs from the application software could cause an action that was not predicted or tested in design. This has some merit, but the probability of it being the cause is small or it's happening again is insignificant. The application software is written in ladder logic which is a high level computer language. It cannot typically be written in such a way as to disable the processor as was evidenced by the lack of a READY light and the loss of the I/O module ACTIVE lights.

A slightly more probable software failure mode involves an error in the internal software logic sometimes called the software kernel. This is the part of the software that interprets the ladder logic code, acquires input data, outputs results of the ladder logic, and diagnoses errors in the hardware and memory. The probability of an error in the software kernel is low. This sequencer has been running at Palisades without error for over six years. The sequencer hardware manufacturer checked their service bulletins and found no relevant notes, cautions, or fixes related to a software kernel problems. The micro-processor portion of the sequencer is a standard Programmable Logic Controller (PLC) that is widely used in various applications in many industries. As such, the PLC manufacturer has the experience and market forces of many PLC owners who would identify that significant common mode failures were a problem with this device. At this time we also do not believe that a common mode software problem exists that would cause the micro-processor to fail.

Plant Response to the Event

Along with the starting of safeguards pumps and opening and closing of valves, it was also noted that the auxiliary feedwater pump (P-8A) and control room HVAC fan (V-95) did not start. Based on design and plant conditions, these devices would not have been expected to start. P-8A did not start since an Auxiliary Feedwater Actuation Signal (AFAS) was not present. V-95 did not start because a load shed signal was not present.

NRC Form 366A
(9-83)

U.S. NUCLEAR REGULATORY COMMISSION
APPROVED OMB NO. 3150-0104
EXPIRES: 8/31/85

LICENSEE EVENT REPORT (LER) TEXT CONTINUATION

FACILITY NAME (1)	DOCKET NUMBER (2)	LER NUMBER (3)					PAGE (4)
		YEAR	–	SEQUENTIAL NUMBER	–	REVISION NUMBER	
Palisades Plant	0 5 0 0 0 2 5 5	9 5	–	0 0 1	–	0 0	0 7 OF 0 8

The condition report also noted that safety injection tank (SIT) pressure control valves (PCV) opened, causing relief valve RV-3161 to relieve to the quench tank (T-73). Based on an evaluation of design and valve lineup, this was correct and is anticipated system behavior.

Evaluations of the above situations are documented with the plant condition report documenting this event.

Corrective Action

1 - The services of the manufacturer of the sequencer hardware will be utilized to diagnose the root cause of the micro-processor module failure.

NRC Form 366A
(9-83)

U.S. NUCLEAR REGULATORY COMMISSION
APPROVED OMB NO. 3150-0104
EXPIRES: 8/31/85

LICENSEE EVENT REPORT (LER) TEXT CONTINUATION

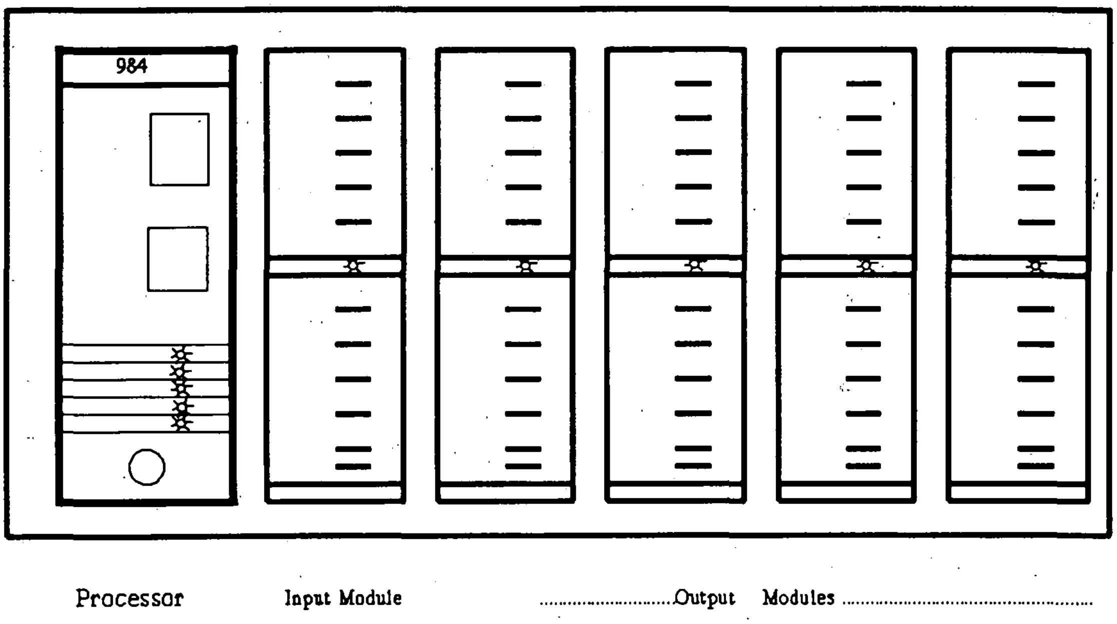
FACILITY NAME (1)	DOCKET NUMBER (2)	LER NUMBER (3)			PAGE (4)
		YEAR	SEQUENTIAL NUMBER	REVISION NUMBER	
Palisades Plant	0 5 0 0 0 2 5 5	9 5	— 0 0 1 —	0 0	0 8 OF 0 8

Attachment 1

Palisades Design Basis Accident (DBA) Sequencer

Facts:
- -Programmable Logic Controller (PLC)
- -Manufactured by Gould Modicon
- -Model 984-380 processor.
- -Series 810 I/O Modules: 1 AC input, 2 AC output, 3 DC output
- -Operates with 115VAC ± 15%, 47 to 63 Hz, Class 1E source (Y30)
- -Takes 5ms/K words of logic to complete scan cycle.
- -Runs self diagnostics on CPU, modules, and memory every scan.
- -Installed in 1988 by FC-737
- -Meets Surge Withstand Capability tests, IEEE 472-1974, ANSI C37.90A-1974

TYPICAL SEQUENCER ARRANGEMENT


984
Processor
Input Module
Output Modules