LICENSEE EVENT REPORT (LER)

| Facility Name (1) | Docket Number (2) | Page (3) |
|---|---|---|
| SAN ONOFRE NUCLEAR GENERATING STATION, UNIT 1 | 0 5 0 0 0 2 0 6 | 1 of 0 7 |

Title (4)

DIESEL GENERATOR LOAD SEQUENCERS UNDERVOLTAGE LOGIC DESIGN DEFICIENCY

| EVENT DATE (5) | | | LER NUMBER (6) | | | REPORT DATE (7) | | | OTHER FACILITIES INVOLVED (8) | |
|---|---|---|---|---|---|---|---|---|---|---|
| Month | Day | Year | Year | /// Sequential Number | /// Revision Number | Month | Day | Year | Facility Names | Docket Number(s) |
| 0 3 | 0 2 | 8 9 | 8 9 | --- 0 0 4 | --- 0 0 | 0 4 | 0 3 | 8 9 | NONE | 0 5 0 0 0 |
| | | | | | | | | | | 0 5 0 0 0 |

| OPERATING MODE (9) | 5 |
|---|---|
| POWER LEVEL (10) | 0 0 0 |

THIS REPORT IS SUBMITTED PURSUANT TO THE REQUIREMENTS OF 10CFR (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) |
| ___ 20.405(a)(1)(iii) | ___ 50.73(a)(2)(i) | ___ 50.73(a)(2)(viii)(A) | |
| ___ 20.405(a)(1)(iv) | X 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 |
|---|---|
| H. E. Morgan, Station Manager | AREA CODE 7 1 4 3 6 8 - 6 2 4 1 |

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

| CAUSE | SYSTEM | COMPONENT | MANUFACTURER | REPORTABLE TO NPRDS | CAUSE | SYSTEM | COMPONENT | MANUFACTURER | REPORTABLE TO NPRDS |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | |
| | | | | | | | | | |

SUPPLEMENTAL REPORT EXPECTED (14)

| | | Expected Submission Date (15) | Month | Day | Year |
|---|---|---|---|---|---|
| ___ Yes (If yes, complete EXPECTED SUBMISSION DATE) | XX NO | | | | |

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


On 3/2/89, with Unit 1 in Mode 5, during a review of a special diesel generator load test, a design deficiency associated with automatic energization of safety-related 4 kV buses in response to a Safety Injection Signal (SIS) concurrent with a Loss of Power (LOP) signal, i.e., SISLOP, was identified. Specifically, when the load sequencers initiate on a SISLOP, the sequencer's LOP latch is reset as soon as the undervoltage (UV) condition on either bus is cleared (i.e., the DG output breaker closes and voltage to the bus is restored). Consequently, if one DG starts and energizes its emergency bus in a shorter period of time than the other DG, the LOP latch in the sequencer associated with the lagging DG will be reset and the output breaker for that DG will not have the required logic to close. As a result, the automatic response capability of one of the two trains of safety-related components during a postulated SISLOP scenario may be lost.

The plant's capability to respond to a LOP concurrent with design basis events was upgraded in 1976 when the sequencers were installed. The design review and design verification testing of the sequencers failed to identify the cross-train reset feature of the LOP latch in the circuit. The root cause is related to deficiencies with engineering review, design basis documentation, and excessive reliance on contractor/vendor engineering support.

Prior to returning Unit 1 to service, time delay relays will be installed in the 4 kV bus UV protective circuits which will ensure that both DG output breakers close before the sequencers' LOP latch is reset. Corrective actions being taken for the root cause concerns are addressed in a 10/3/88 submittal to the NRC regarding SCE's assessment of engineering and technical support for San Onofre.




IE22

1/1

Plant: San Onofre Nuclear Generating Station
Unit: One
Reactor Vendor: Westinghouse
Event Date: March 2, 1989

A. CONDITIONS AT TIME OF THE EVENT:

Mode 5 (Cold Shutdown) during the Cycle X refueling outage.

B. BACKGROUND INFORMATION:

Unit 1 is provided with two independent Class 1E 4160 Volt (4 kV) AC electrical distribution systems (Bus 1C and 2C)(EIIS System Code EB) which supply electrical power to systems and components that are required for normal operation, for safe plant shutdown and for mitigating the consequences of Design Basis Events. These two 4 kV distribution systems are normally energized by off-site electrical sources.

In the event that electrical power is not available from the off-site sources, each of the two 4 kV distribution systems is powered by an emergency Diesel Generator (EIIS Component Code DG)(EIIS System Code EK). The Safeguard Load Sequencing Systems (SLSS), also called Sequencers, are designed to automatically start the emergency Diesel Generators (DG) upon a Safety Injection Signal (SIS), a Loss of Bus (LOB) signal or a Loss of Power (LOP) signal.

LOP is initiated by the sequencers when an undervoltage (UV) condition is sensed on both 4 kV safety buses. The UV inputs to the Sequencers are provided by four UV relays (two per 4 kV safety bus) through eight auxiliary relays (EIIS Component Code 27). Each sequencer, therefore, receives two auxiliary UV relay inputs from its own train 4 kV bus and two from the cross-train bus. The sequencers' logic is configured so that a LOP latch is set when an UV condition is sensed on both buses by at least 1 of 2 auxiliary relays on each bus. The LOP latch is reset when the UV condition is cleared on either bus.

Upon a SIS with a LOP signal present (i.e. SISLOP), the Sequencers start their respective DGs, close the DG output breakers once the DGs attain proper voltage and frequency, and sequentially load their respective safety-related buses.

C. DESCRIPTION OF THE EVENT:

1. Event:

On April 27, 1989, a special test was conducted to verify proper loading of DG No. 2. On March 3, 1989, following a review of this special test, a design deficiency associated with automatic energization of safety related 4 kV buses in the event of a SISLOP was identified. Specifically, when the sequencers initiate on a SISLOP, the sequencer's LOP latch is reset as soon as the UV condition on either bus is cleared (i.e., the DG output breaker closes and voltage to the bus is restored). Consequently, if one DG starts and energizes its emergency bus in a shorter period of time than the other DG, the LOP latch in both sequencers will be reset and the output breaker

for the lagging DG will not have the required logic to close. Based upon the data associated with the actuation time of the bus UV relays, it is necessary for the output breaker of the lagging DG to close within approximately 0.8 seconds of the leading DG. If the lagging DG output breaker does not close within this time frame during a postulated SISLOP scenario, the automatic response capability of the safety-related components powered by the lagging DG would be lost.

2. Inoperable Structures, Systems or Components that Contributed to the Event:

None.

3. Sequence of Events:

Not applicable.

4. Method of Discovery:

This deficiency was discovered on March 2, 1989 while evaluating the results of a special test. This test, which was conducted on February 27, 1989, involved the loading of DG No. 2 onto 4 kV Bus 2C to demonstrate emergency DG operation and load capacity subsequent to various plant changes. The test consisted of utilizing Sequencer manual initiate switches to simulate a SISLOP. The SIS and LOP switches were actuated and released, resulting in the expected SISLOP initiation. After SISLOP initiation, the DG accelerated to operating speed, but the output breaker did not close as expected. During the subsequent investigation, it was discovered that release of the LOP switch allowed a reset of the Sequencer LOP latch by the UV relays on the cross-train 4 kV Bus 1C which was still energized per test conditions. Resetting the LOP latch prevented the closure of the DG output breaker. Additional review of the sequencer logic diagrams revealed that the LOP latch would reset anytime that either safety bus was re-energized.

5. Personnel Actions and Analysis of Actions:

Not applicable.

6. Safety System Responses:

Not applicable.

D. CAUSE OF THE EVENT:

1. Immediate Cause:

The plant's capability to respond to a LOP concurrent with design basis events was upgraded in 1976 when the SLSS trains were installed. The design review and design verification testing of the sequencers failed to identify the cross-train reset feature of the LOP latch in the circuit.

2. Root Cause:

SCE's root cause investigation of this design deficiency has been completed. Final findings are that the root cause is related to weaknesses within the design process and post-modification testing programs. Although a specific root cause cannot be determined, SCE believes that the root cause is bounded by the one or more of the general engineering deficiencies previously described in an October 3, 1988 submittal to the NRC regarding SCE's assessment of engineering and technical support for San Onofre. It is believed that these general engineering deficiencies are applicable to this LER as follows:

a. Opportunities to detect the design deficiency were missed due to a failure by Engineering to fully recognize and question the system design basis, assumptions and system interactions. This deficiency also affected the adequacy of the design verification testing which failed to verify the performance of the sequencers under all credible operating scenarios, including possible time differences between DG train responses.

b. At the time that the sequencer was designed, there were no programmatic requirements for the development, update, compilation, review or verification of design basis documents.

c. At the time of sequencer design, SCE placed excessive reliance on the sequencer vendor to verify compliance with design requirements and design bases. The sequencer is a custom designed Class 1E Engineered Safety Features Actuation System. SCE relied on the vendor, based on their past experience with Class 1E ESF systems, to engineer, fabricate and test a system meeting specific SONGS 1 requirements. It was expected that the vendor would consider system interactions and ensure that the sequencers were engineered to perform as required under all postulated scenarios. SCE's level of engineering review at the time was not adequate to detect the identified design deficiency.

E. CORRECTIVE ACTIONS:

1. Corrective Actions Taken:

The following corrective actions being taken for the root cause concerns are addressed in an October 3, 1988 submittal to the NRC regarding SCE's assessment of engineering and technical support for San Onofre.

a. A training program for supervisory personnel performing review of technical and engineering work, has been initiated. This program addresses, in part, the responsibilities of technical reviewers and emphasizes the need to foster a questioning attitude to ensure poor quality work is identified during the design review process. Additionally, a discipline system engineering approach has been established for the organization of the design engineering staff in order to develop a detailed knowledge of system design and operational requirements.

b. In addition to increasing the level of SCE engineering personnel involvement in the design of the plants as discussed above, SCE engineering personnel are increasing their oversight of vendor performance and contractor engineering support.

c. A design basis documentation program has been established to capture and maintain the design basis for Units 1, 2 and 3. The SONGS 1 sequencer design basis is currently being developed and is scheduled for completion by December 30, 1989.

2. Planned Corrective Actions:

a. Time delay relays (EIIS Component Code 2) will be installed prior to return to service. The relays will be in the cross-train UV inputs to the sequencers for monitoring LOP conditions. The time delay relays will be continuously energized during normal voltage conditions. The relays will drop out instantaneously upon receipt of an UV signal and will pick up 12 seconds after restoration of bus voltage. The 12 second time delay will ensure that both DG breakers close before reset of the opposite train undervoltage signal to each sequencer occurs.

b. In addition to the above discussed training program, training programs will be developed and implemented for the design engineering staff which will provide:

i) Technical training on specific systems coupled with an integrated system knowledge of plant design and operation.

ii) Training to develop the capability to critically examine data, recommendations, etc.

iii) Cross-training for engineers and supervision will be offered as a career enhancement opportunity for personnel in the site and design organizations. Such cross-training will improve communications and enhance understanding of the functions, needs and perspectives of the organizations involved.

F. SAFETY SIGNIFICANCE OF THE EVENT:

For a SISLOP event, at least one train of safeguards is required to place the plant in a safe shutdown condition. The deficiency described in this report could have resulted in one of the two trains of safeguards being unavailable for automatic actuation. This deficiency is safety significant only in the event that a safety related component associated with the leading DG fails. In the event of a single failure of the Safety Injection train which receives power from the loaded diesel, neither train of safety injection would have been automatically actuated as assumed in the transient analyses. Since the lagging DG would have received a start signal and would therefore be running, upon recognition of the deficiency, operator action could be taken to manually energize the bus and start required safety equipment.

G. ADDITIONAL INFORMATION:

1. Component Failure Information:

Not applicable

2. Previous LERs for Similar Events:

Recent LERs reporting similar design and design control related conditions:

Unit 1 (Docket No. 50-206)

LER 1-86-007, Revision 1, reported a single failure susceptibility of the Reactor Protection System.

LER 1-87-015 reported that certain systems were susceptible to single failure.

LER 1-88-001 reported that several components requiring environmental qualification were not included in the administrative controls for the environmentally qualified equipment. Additionally, other components were found to be in an unqualified configuration.

LER 1-88-006, Revision 1, reported a condition where the Unit 1 Backup Nitrogen Systems (as designed, installed and operated) did not satisfy the licensing and design basis for the systems.

LER 1-88-009 reported a condition in which the emergency diesel generators could have exceeded an intended electrical load limit.

LER 1-88-016 reported a condition in which the south refueling water pump may not have started as required due to a wiring discrepancy.

LER 1-88-017 reported a condition in which the auxiliary feedwater storage tank minimum volume requirements for accident mitigation may have been inadequate.

LER 1-88-019 reported that design deficiencies existed in automatic controls of the electrical power distribution system.

LER 1-88-020 reported that design requirements of NUREG-0737 had not been fully implemented in the design of the steam generator wide-range level indication system.

LER 1-89-003 reported a condition in which the failure mode of Component Cooling Water Valves was non-conservative with respect to design requirements due to inadequate single failure analysis.

LER 1-89-007 reported a single failure susceptibility of Reactor Protection System features credited for diverse Reactor Coolant Pump (RCP) locked rotor protection.

Unit 2 (Docket No. 50-361)

LER 2-88-008, Revision 1, reported various conditions resulting in the Component Cooling Water System being outside its design basis due to design control program deficiencies.

LER 2-88-010 reported a condition in which both emergency chillers were rendered inoperable as a result of not addressing freon level as a critical design parameter.

LER 2-88-017 reported that a spent fuel pool siphon event occurred as a result of the failure to identify and implement the design intent to utilize administrative controls on certain locked valves.

LER 2-88-034 reported a condition involving safety related Component Cooling Water System valves being susceptible to seismically-induced common mode failures.

3. Results of NPRDS Search:

Not applicable.

*Southern California Edison Company*

SAN ONOFRE NUCLEAR GENERATING STATION

P. O. BOX 128

SAN CLEMENTE, CALIFORNIA 92672

H. E. MORGAN
STATION MANAGER

TELEPHONE
(714) 368-6241

April 3, 1989

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

Subject: Docket No. 50-206
30-Day Report
Licensee Event Report No. 89-004
San Onofre Nuclear Generating Station, Unit 1

Pursuant to 10 CFR 50.73(a)(2)(ii), this submittal provides the required 30-day written Licensee Event Report (LER) for an occurrence involving the Safeguards Load Sequencing System. Neither the health and safety of plant personnel or the public was affected by this occurrence.

If you require any additional information, please so advise.

Sincerely,

H E Morgan

Enclosure: LER No. 89-004

cc: F. R. Huey (USNRC Senior Resident Inspector, Units 1, 2 and 3)

J. B. Martin (Regional Administrator, USNRC Region V)

Institute of Nuclear Power Operations (INPO)

IE22
1/1