LICENSEE EVENT REPORT (LER)

FACILITY NAME (1)	DOCKET NUMBER (2)	PAGE (3)
DIABLO CANYON UNIT 1	0 5 0 0 0 2 7 5	1 OF 9

TITLE (4) TECHNICAL SPECIFICATIONS 3.3.3.8 AND 3.7.10 NOT MET DUE TO PROCEDURAL DEFICIENCY

EVENT DATE (5)			LER NUMBER (6)			REPORT DATE (7)			OTHER FACILITIES INVOLVED (8)	
MON	DAY	YR	YR	SEQUENTIAL NUMBER	REVISION NUMBER	MON	DAY	YR	FACILITY NAMES	DOCKET NUMBER (8)
10	01	92	92	- 0 2 8 -	0 1	05	20	93	DIABLO CANYON UNIT 2	0 5 0 0 0 3 2 3

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

THIS REPORT IS SUBMITTED PURSUANT TO THE REQUIREMENTS OF 10 CFR: (11)

X 10 CFR 50.73(a)(2)(i)(B)

OTHER - (Specify in Abstract below and in text, NRC Form 366A)

LICENSEE CONTACT FOR THIS LER (12)

NAME	TELEPHONE NUMBER AREA CODE	TELEPHONE NUMBER
DAVID P. SISK, SENIOR REGULATORY COMPLIANCE ENGINEER	805	545-4420

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	
X	I C	C P U	H 2 6 0	N							

SUPPLEMENTAL REPORT EXPECTED (14)		EXPECTED SUBMISSION DATE (15)	MONTH	DAY	YEAR
| | YES (if yes, complete EXPECTED SUBMISSION DATE)	| X | NO				

ABSTRACT (16)

On October 1, 1992, at 0731 PDT, with Unit 1 in Mode 6 (Refueling) and Unit 2 in Mode 1 (Power Operation) at 100 percent power, and on November 26, 1992, at 1948 PST, with Units 1 and 2 in Mode 1 at 100 percent power, Technical Specification (TS) 3.3.3.8 and 3.7.10 Action Statements were not met when the fire protection system (FPS) computer was inoperable for more than one hour without the required compensatory measure established.

On November 26, 1992, at 1848 PST, the FPS computer malfunctioned, making the FPS inoperable and requiring compensatory fire watches in accordance with TS 3.3.3.8 and 3.7.10. However, the computer malfunction was not identified until November 27, 1992, at 0902 PST and compensatory measures were immediately established. On December 4, 1992, a review of records identified that a similar reportable event had occurred on October 1, 1992, at 0731 PDT.

The root cause of these events was lack of adequate procedures/instructions to configure the data sensing software in the FPS computer.

To prevent recurrence, a procedure for disabling the data retrieval points on the FPS computer will be developed. In addition, a Software Quality Assurance Plan, which includes Configuration Management for the FPS computer, is being implemented.

I. Plant Conditions

Event 1 (October 1, 1992). Unit 1 was in Mode 6 (Refueling) and Unit 2 was in Mode 1 (Power Operation) at 100 percent power.

Event 2 (November 26, 1992). Units 1 and 2 were in Mode 1 (Power Operation) at 100 percent power.

II. Description of Event

A. Summary:

Event 1 On October 1, 1992, at approximately 0631 PDT, the fire protection system (FPS) computer (IC)(CPU) malfunctioned and disabled the audible fire alarm (IC)(FRA) in the control room (NA). At 0731 PDT, Technical Specification (TS) 3.3.3.8 and 3.7.10 Action Statement requirements were exceeded when the FPS computer was inoperable for more than one hour without the required compensatory measures established. The computer malfunction had not been identified and fire watch compensatory measures had not been implemented. Therefore, TS 3.3.3.8 and 3.7.10 were not met.

Event 2 On November 26, 1992, at 1848 PST, the FPS computer malfunctioned and disabled the fire alarm system (IC). At 1948 PST, the Action Statement requirements for TS 3.3.3.8 and 3.7.10 were exceeded when the FPS computer was inoperable for more than one hour without the required compensatory measures established. The computer malfunction had not been previously identified and fire watch compensatory measures had not been implemented. Therefore, TS 3.3.3.8 and 3.7.10 were not met.

B. Background:

TS 3.3.3.8 Action Statement a. requires that, with the number of operable fire protection instruments less than the minimum required by Table 3.3-11, within one hour establish a fire watch patrol to inspect the zone(s) with the inoperable instruments at least once per hour.

TS 3.7.10 requires that fire barrier penetrations in the fire area boundaries protecting safety-related areas be functional whenever the equipment protected by the fire barrier penetrations is required to be operable. With one or more required fire barrier penetrations nonfunctional, within one hour either establish a continuous fire watch on at least one side of the affected penetration or verify the operability of the smoke detectors (IC)(DET) on at least one side of the nonfunctional fire barrier and establish an hourly fire watch patrol.

The FPS at Diablo Canyon Power Plant (DCPP) is comprised of individual detectors grouped into zones and a set of centralized alarm panels (IC)(ALM)(PL) located within the control room. When an individual detector alarm is activated, the signal is received by the alarm panel and associated indicator lights illuminate for the affected zone. The signal is also fed to data gathering panel FS-90 (IC)(DAL)(PL). The FS-90 panel consolidate the alarm signals. The alarm signals are then communicated from the FS-90 panel to the Gateway central communication microprocessor. When the central communication microprocessor receives an alarm signal, an audible alarm and the main annunciator window (ANN)(WIN) are activated to alert the control room operators.

When no alarm is present, programming within the system ensures that the FS-90 panels and the central communication microprocessor are in communication with each other. If there is a breakdown in communication between these two types of devices, an audible alarm is sounded in the control room and the FS-90 panels revert to a "stand alone" mode. This "stand alone" mode function allows the FS-90 panels and their associated detectors to function as an independent unit. If one of the FS-90 panels receives a signal from a detector while in the "stand alone" mode, the FS-90 panels would respond with a local audible alarm and individual indicator lights in the control room to alert the operators.

If the central communication microprocessor is rebooted, there is a temporary loss of communication between the FS-90 panels and the central communication microprocessor. This results in an audible alarm due to the "stand alone" function and is either acknowledged by the operators and reset or allowed to alarm briefly while the central communication microprocessor re-initializes and re-establishes communication with the FS-90 panels, at which point the alarm ceases.

C. Event Description:

Prior to Event 1, on October 1, 1992, at approximately 0000 PDT, the FPS computer was shut down to switch power supplies (JX) in preparation for a routine 480V Bus 1H (ED)(BU) outage. At approximately 0141 PDT, with the power restored, the FPS computer automatically rebooted, restoring normal system operation. The fire system operability was confirmed by observing annunciator (ANN) responses during a "smoke test" of the detectors.

Event 1 On October 1, 1992, at approximately 0631 PDT, the Gateway central communication microprocessor malfunctioned during the generation of a routine end-of-shift report without the trouble alarm annunciating or the FS-90 panels sensing the malfunction and reverting to the "stand alone" mode. The malfunction inhibited the ability for detection alarm signals to annunciate on the control room main annunciator system.

At 0731 PDT, the Limiting Conditions for Operation (LCOs) for TS 3.3.3.8 and 3.7.10 were exceeded when the FPS computer was inoperable for more than one hour without the required compensatory actions established.

At 0800 PDT, the event was identified by the system engineer during a subsequent review of the computer printout. The Gateway central communication microprocessor was cold rebooted and normal system operation was restored.

At the time, the FPS computer manufacturer (Honeywell) was contacted concerning this event; Honeywell reported that this was a known condition and that this condition would cause an inability of the computer to query the status of detection and sensor points, but would still allow incoming alarms to activate the main annunciator. Honeywell stated at the time that this condition had been identified at other installations and that they would be providing some replacement of components to prevent this condition from recurring. Therefore, PG&E was led to believe that the FPS was operable during this time and that no compensatory fire watch was required.

Prior to Event 2, on November 26, 1992, at 1046 PST, the PK 10-15 annunciator indicated an FPS trouble alarm. The FPS computer in the control room performed an automatic system reboot due to a spurious interrupt, as indicated by a message on the printer (PRNT). However, there were no indications of a power spike or interrupt present. The Gateway central communication microprocessor automatically rebooted, but inexplicably did not cause the audible alarms that are normally associated with a system reboot. It appears that the FS-90 panels did not terminate communication with the Gateway central communication microprocessor and switch to the "stand alone" mode.

The FPS computer was then verified to respond to alarms by initiating a trouble alarm to the FPS computer and observing the response by the control room annunciator. Therefore, at 1300 PST, all indications were that the FPS computer had successfully rebooted automatically.

Event 2 On November 26, 1992 at 1848 PST, the Gateway central communication microprocessor again malfunctioned during the generation of a routine end-of-shift report without the trouble alarm annunciating or the FS-90 panels sensing the malfunction and reverting to the "stand alone" mode. The malfunction inhibited the ability for detection alarm signals to annunciate on the control room main annunciator system. This was evident by a subsequent review of the computer printout. The required compensatory measure for a Gateway failure of this type (either planned or discovered), would be to station a continuous fire watch at the FS-90 panels so that an inaudible alarm at these panels would be identified and control room

operators would be immediately alerted to the condition.

At 1948 PST, the LCOs for TS 3.3.3.8 and 3.7.10 were exceeded when the FPS computer was inoperable for more than one hour without the required compensatory actions established.

On November 27, 1992, at 0902 PST, Event 2 was identified during the performance of Surveillance Test Procedure (STP) M-64, "Deluge System Functional Test." The expected annunciator alarms were not received during the test and a continuous fire watch was immediately established. At approximately 1030 PST, as an investigative measure, a detector was "smoke tested." The computer malfunction was confirmed to have rendered the detection annunciator inoperable; therefore, the earlier Honeywell claims regarding the nature of this problem were incorrect, or the problem was different than that previously identified by Honeywell. A cold reboot of the computer was performed and the system appeared to reboot successfully, restoring normal system operation. At 1059 PST, the Unit 1 Smoke Detector 15-21 was activated to verify the system operation and the fire watch was discontinued at 1105 PST.

On December 1, 1992, at 0900 PST, an hourly fire watch was established in the control room as a conservative measure to visually check the fire panels for any alarms. Immediate corrective actions have been implemented and the system is now fully functional, but as a prudent action this hourly control-room fire watch will remain in place until the corrective actions to prevent recurrence are implemented.

On December 4, 1992, a Technical Review Group (TRG) determined that TS 3.3.3.8 and 3.7.10 had not been met for Event 1 and, therefore, that Event 1 also was reportable.

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

None.

E. Dates and Approximate Times for Major Occurrences:

1.	October 1, 1992, at 0631 PDT:	The FPS computer malfunctioned.
2.	October 1, 1992, at 0731 PDT:	Event 1. The one-hour Action Statement requirements for TS 3.3.3.8 and 3.7.10 were exceeded.
3.	October 1, 1992, at 0800 PDT:	The FPS computer was rebooted.

4. November 26, 1992, at 1848 PST: The FPS computer malfunctioned.

5. November 26, 1992, at 1948 PST: Event 2. The one-hour Action Statement requirements for TS 3.3.3.8 and 3.7.10 were exceeded.

6. November 27, 1992, at 0902 PST: Event 2 discovery date; a continuous fire watch was established.

7. December 4, 1992: Event 1 discovery date; the TRG determined that Event 1 was also reportable.

F. Other Systems or Secondary Functions Affected:

None.

G. Method of Discovery:

While performing STP M-64, a Unit 2 control room operator identified that the main annunciator was not responding to the anticipated fire system alarms (Event 2). A subsequent review of previous computer failures identified one similar occurrence (Event 1).

H. Operator Actions:

Event 1. None.

Event 2. Control room personnel established a continuous fire watch at the fire alarm panels in the control room.

I. Safety System Responses:

None required.

III. Cause of the Event

A. Immediate Cause:

For both Events 1 and 2, the FPS computer malfunctioned.

B. Root Cause:

Investigation of the failures of the FPS computer was performed to determine the reason for the problem. An attempt to intentionally duplicate the failure of the computer was conducted. The computer did

fail in a similar manner and the data were collected from the computer files and computer printer logs. Discussions with Honeywell confirmed that a loss of configuration control had occurred between various Honeywell corporate departments during the final stages of startup testing and turnover. The FPS computer software was a later revision than the one indicated in the files maintained by Honeywell. A possible hardware and software revision incompatibility had been identified by Honeywell that had resulted in a failure similar to that experienced by DCPP. The normal bulletins at Honeywell are internal field technician documents that would not normally be distributed to system owners; however, this problem resulted in a mandatory upgrade that was made available to all known owners with this specific software version. Since Honeywell was not aware that PG&E had a later software version, PG&E was not provided with this upgrade.

During trouble shooting, the Honeywell technician identified an off-normal condition involving the disabling of the data gathering panel for the I&C/medical facility. To completely disable the panel, all points on the panel must be disabled to prevent the report or inquiry functions from "hanging up" while looking for nonexistent data. This had been done prior to initial turnover to Operations, but operating personnel were not aware of this requirement. When the software was reloaded subsequent to a hard drive failure in 1992, only the panel was disabled, not the specific data gathering points. With proper disabling of the I&C building data gathering panel, the computer continues to operate properly.

Based on the above investigation, the root cause of these events has been determined to be procedural deficiency, in that the consolidated FPS computer instructions for configuring the data sensing software were inadequate.

C. Contributory Cause:

One of the contributing causes of this event is inadequate software configuration control by PG&E. In early 1990, a Software Quality Assurance (SQA) plan was developed to create configuration control programs for all the computer systems on site. The computer was included in this program, but an implementation schedule was not developed.

IV. Analysis of the Event

Although the compensatory measures required by the TS were not continuously in place while fire barriers were impaired, the impaired condition did not represent a significant safety concern due to the conservative design features and procedural controls inherent in the DCPP fire protection program.

All activities throughout the plant are strictly controlled administratively, in practice of the "defense-in-depth" concepts, to ensure that the highest level of fire protection safety is maintained at all times. All work orders are reviewed by the fire protection specialists to ensure that appropriate compensatory measures are implemented for activities which may impact the overall effectiveness of the DCPP fire protection program. Nuclear Plant Administrative Procedure C-13, "Fire Loss Prevention," governs the program, and includes controls for open flame and welding processes, the use and control of flammable liquids, and the control of transient combustibles.

In addition to the administrative controls used to minimize the risk of a fire during day-to-day activities, the potential for spread of fire is reduced due to the general layout and construction features of the plant. Walls, floors, and ceilings are constructed of noncombustible materials, and physical separation (distance or fire barriers) is provided between potential hazards. Where possible, extensive usage of conduits was made in lieu of cable trays to keep exposed combustibles to a minimum.

Where warranted, automatic suppression systems are provided in areas with potential fire hazards or equipment required for safe shutdown is located. In addition, manual fire fighting equipment, such as portable extinguishers (KQ) and hose reels (HR), are strategically located throughout the plant for immediate use by the fire brigade. DCPP maintains a fully staffed fire brigade, which receives periodic training to respond rapidly and effectively to fires. Furthermore, as part of the General Employee Training program , all employees are trained in identifying and reporting fires and potential fires at DCPP.

The nature of the barrier impairments are also such that they would not render the fire barriers totally ineffective. In general, the barrier impairments resulted from inoperable penetration seals within the fire barrier. While the degraded portion of the barriers could not be relied upon in limiting the spread of a fire, the remainder of the barriers would still provide a tortuous path for propagating a fire.

CONCLUSION

Based on the low combustible loadings within the plant, the administrative procedures in controlling combustibles and ignition sources, the building layout and construction features, and the fire protection features provided for identifying and suppressing fires quickly, a postulated fire anywhere in the plant is not likely to sustain itself much less propagate across any of the noted barrier impairments.

Thus the health and safety of the public were not affected by these events.

V. Corrective Actions

A. Immediate Corrective Actions:

Following the November 26, 1992 event, the FPS computer was cold rebooted, the system was verified to operate satisfactorily, and a fire watch was established in the control room as a conservative measure until the reliability of the computer was re-established.

B. Corrective Actions to Prevent Recurrence:

1. An SQA Plan, which includes Configuration Management for the FPS computer, is being implemented.

2. A procedure for disabling the data retrieval points on the FPS computer will be developed.

VI. Additional Information

A. Failed Components:

1. Component: FPS computer.

2. Manufacturer: Honeywell.

3. Model number: Deltanet micro Central/Excel plus with model W7053 Gateway.

B. Previous LERs on Similar Problems:

None.