ENCLOSURE 1

REVIEW OF THE DCPRA: LETTER REPORT-07/REV.1

A REVIEW OF SYSTEM ANALYSIS IN THE DCPRA: DIESEL GENERATOR AND DIESEL FUEL TRANSFER SYSTEMS

G. Bozoki
R. Fitzpatrick
M. Sabek

July 1989

Risk Evaluation Group
Department of Nuclear Energy
Brookhaven National Laboratory
Upton, NY 11973

Prepared for
U.S. Nuclear Regulatory Commission
Washington, DC 20555
Contract No. DE-AC02-76CH00016
FIN A-3958

1. INTRODUCTION

1.1 Objectives

The main objective of this letter report is to summarize the results, to date, of reviewing the unavailability analysis of the Diesel Generator and Diesel Fuel Transfer Systems described in the DCPRA.[1] The review was carried out with special attention to the details of the unavailability modelling of the maintenance activities on the DGs. (This particular emphasis was prompted by a request of the Pacific Gas and Electric Co to change the Allowed Outage Time (AOT) of the DGs from the present outage of three days to seven days, and the fact that the study[2] supporting this request derived data on expected core damage frequency changes based mainly on the DCPRA.) This report reflects BNL's current understanding of the subject systems and as such must be considered interim results. Final results will be provided in the NUREG/CR to be issued at the end of the project. That will reflect, at that time, any additional supporting input submitted by PG&E as well as any direct feedback on these preliminary findings.

1.2 Organization of the Report

Section 2 provides condensed descriptions about the configurations and functions of the Diesel Generator and the Diesel Fuel Oil Transfer Systems. It also describes the dependency of these systems on support equipment, the surveillance and maintenance conditions, the unavailability modelling in the DCPRA, and the original PRA results. The purpose of this approach is to present the reader stand alone documentation to which the review's findings can be directly compared. Section 3 contains the results of the BNL review and presents the current preliminary findings.

For completeness, the ranked cut sets of hardware unavailabilities (both independent and total) obtained by BNL for various diesel configurations are given in Appendix A.

2. UNAVAILABILITY MODELLING OF THE DIESEL GENERATOR AND DIESEL FUEL OIL TRANSFER SYSTEMS

2.1 Diesel Generator System Description, Configurations and Functions

The Diesel Generator System at the Diablo Canyon plant consists of five diesel generators: two dedicated to Unit 1, two dedicated to Unit 2, and one (a "swing diesel") shared between the two units. According to the DCFSAR,[3] the individual diesel generator units are isolated from each other and from other equipment. The swing diesel is physically located in Unit 1. Each diesel generator supplies power to its associated 4.16kV vital bus (H, G, and F - Units 1 and 2). In the event of a loss of electrical power from the main generator (due to a unit trip, a safeguard signal or a loss of voltage on a vital bus) the vital 4.16kV buses are automatically disconnected from the main generator and transferred to the offsite standby source. (The Unit 1 main generator provides power through auxiliary transformer 12. The standby power is provided through startup transformers 11 and 12.) If this transfer is unsuccessful or the standby power is unavailable, the diesel generators must start and provide power to the affected buses. The diesel generators start on undervoltage signals from their respective buses, load onto those buses (the output breakers are normally open), initiate reloading of the vital loads and continue delivering power at normal frequency to the buses. A safety injection actuation signal (SIS) from either Train A or B of the SSP System will also start the diesels (Train A will start 11 and 13, Train B will start 11 and 12).

The swing diesel (13) may supply power to either Unit 1 or Unit 2 vital Bus F. It will start with an undervoltage or an SI signal from either unit (SSPS Train A). Because the output is not shared simultaneously by the units, only one of its two circuit breakers is closed at a time. The breakers have individual sets of control and protection circuits. If one of the units receives an SI signal (earlier than the other), it is given priority of using the swing diesel.

The DGs are 2750 kW, 18 cylinder, vee configuration, ALCO made units. Each unit consists of a self-contained diesel engine directly connected to an alternating current generator. Each diesel has dual train electrical starting circuits and air system with turbocharger, ventilation, fuel oil system, self-contained radiator cooled jacket cooling water system, lube oil system, and speed control governor system.

- Each independent starting circuit has its own dc power source (DG11; dc panels 13, 12. DG12; dc panels 12, 11. DG13; dc panels 11, 13. DG21; dc panels 22, 21. DG22; dc panels 23, 22). The operating control circuit is common. Without control power a unit keeps running. A mechanical trip handle, located in the diesel compartment serves to shut the unit down.

- The air start system consists of two trains. Each train includes a compressor, a dryer, an air receiver and two air-driven motors. Air from receivers is fed through regulator valves and up to the starting air system solenoid valves. Only one motor is needed to start a diesel. Power supply to the compressor trains are provided by 480V ac buses: [DG11; Trains A and B; 1H, 1G. DG12; Trains A and B; 1G, 1F. DG13; Trains A and B; 1F (backup 2F), 1H (backup 2F). DG21; Trains A and B; 2G, 2F. DG22; Trains A and B; 2H, 2G.] One solenoid control valve of an air driven motor in each compressor train gets its "open" signal from the normal control, the other solenoid valve receives signal from the backup control. Upon initiation of a start, the solenoid valves open supplying air to the motors. After initiation, pressure switches located on the discharge of the jacket water pump shuts off the air supply. The air start system supplies air to the Level Control Valves (LCVs) of the diesel fuel oil day tanks. There is one air supply line per LCV.

- The air start system also includes an air operated turbocharger for quick starting and load pickup. The associated air subsystem consists of one turbo air compressor, one starting air receiver tank, and an air dryer. Two solenoid operated shutoff valves, one on each of the two supply lines, control the air supply to the turbocharger. A solid state speed-loss sensor

controls the turbo-assist air supply to prevent a critical loss of speed when a sudden large load increase occurs.

- Each diesel has also another air system: the combustion air and exhaust system (ventilation), containing the intake and exhaust silencers and the two motor-driven crankcase exhauster fans.

- The engine fuel oil system involves the fuel oil day tank. Fuel oil is supplied by the Diesel Fuel Oil Transfer System (see its description in Section 2.2). The fuel oil level in the day tank is controlled by two redundant level control valves (LCVs). Each LCV has two 480V ac control power sources; a normal supply and a backup supply. The power sources for LCVs associated with the primary fuel oil transfer pump (Train 02) are: 480V ac buses 1G and 2G. Power sources for LCVs associated with the secondary fuel oil transfer pumps (Train 01) are: 480V ac buses, 2H and 1H. The valves may be actuated also manually.

- The cooling of a diesel unit is provided by a closed loop jacket cooling water system. The jacket water pump takes water from the lube oil cooler and the turbocharger aftercooler. There is a 50-gallon expansion tank connected to the suction side of the pump. The pump discharges water through the engine block and turbocharger to a common return line. Engine water temperature is maintained at 170°F by a thermostatically controlled three-way valve set. Overheated water is sent to a water radiator, where it is cooled by forced air (engine driven fan) taken from outside the building.

- The lubricating oil system consists of an oil reservoir, an engine driven pump and a heat exchanger. The heat exchanger is cooled by the engine jacket cooling water system. Lubricating oil temperature is thermostatically controlled. The oil is kept in the range of 90°-110°F circulated by a small pre-circulation pump even if the generator is idle, to reduce wear during the engine start period. The diesel automatically stops if the oil pressure drops below 40 psig.

- To control the fuel delivery and therefore the engine's speed and generator output frequency to a predetermined value, an engine governor speed control unit is used. The governor has electrical and mechanical controls; both of which act through a hydraulic actuator to control the fuel supply.

The diesels cannot respond to a start signal under the following conditions:

1. Shutdown relay tripped.
2. Manual test condition.
3. Low fuel level in the day tank.
4. Low pressure in both starting air receivers.
5. Loss of dc control power.
6. Voltage regulator on manual.

The eventual problems of the diesels are annunciated by various alarms (14 groups of signals) in the control room.

The loads of the diesels are listed in Table 2.1. Each diesel has enough capacity to handle some extra startup load. The loading of the diesels during the recirculation phase of a LOCA is under the control of the operator.

Each generator compartment is provided with an automatic flooding CO_2 gas system for fire protection.

2.2 Diesel Fuel Oil Transfer System, Configuration and Function

The diesel fuel oil transfer system maintains a supply of fuel oil to each DG day tank from two large underground storage tanks (capacity: 40,000 gallons per tank). It contains two trains (01 and 02), each having a rotary screw type positive displacement pump. These pumps are self priming. A single pump has enough capacity (55 gpm at 50 psig) to supply all the five diesels. (The fuel consumption rate is about 3.2 gpm per DG). Each pump train has a fuel oil distribution header supplying all five of the DGs.

Manual crosstie valving between headers allow either transfer pump to deliver to either header. Also, it is possible to pump from either of the storage tanks.

Local controls for the system are located at each DG. There are two sets of controls; one for pump train 01 and another for pump train 02. These are the LCV switches: a total of 10 (5x2). Each switch starts the transfer pumps and opens the LCV of its respective train. The pump start levels are different: 252 gallons for train 01 and 271 gallons for train 02. Once a pump is started it will remain running until shut down by the operator. If all the LCVs are closed (the day tanks are full) the fuel oil will recirculate back to the main storage tank.

The motors that drive the pumps are powered by 480V vital ac buses (pump train 01 by either bus 1H or 2H, from Units 1 and 2 respectively, and pump train 02 by either bus 1G or 2G). A manual transfer switch determines the alignment, the only criterion for alignment is that the pumps should be powered by different units.

The operation of the oil fuel transfer system is made on a demand basis: when one of the day tanks reaches a low level set point, the fuel transfer pumps start and remain running until all diesels have been shut down. For the six hour mission time (24 hours for seismic events) of the diesels, the fuel transfer system must remain functioning to replenish the fuel supply to each running diesel. The minimum total storage in the storage tanks is sufficient for seven days of power generation.

The importance of the operability of the fuel oil transfer system for the plant safety is obvious: if the fuel transfer system is unavailable, it results in failure of all the DGs of both units, Unit 1 and Unit 2. For events when both ac powered fuel transfer pumps might become unavailable, a dedicated portable fuel oil driven pump is kept at hand. This pump takes suction directly from the main storage tank and connects to one of the fuel

delivery headers. Flexible hoses are used to make the appropriate connections.

2.3 Top Event Definitions, Success Criteria

Associated with the unavailability of the diesel generators, the DCPRA defines six top events in the electric part of the support system event tree. The designators of these top events and their relationships with the diesels are:

- Top Event GF - Diesel Generator 13 ("swing diesel")
- Top Event GG - Diesel Generator 12
- Top Event GH - Diesel Generator 11
- Top Event 2G - Diesel Generator 21
- Top Event 2H - Diesel Generator 22
- Top Event SW - Units alignment of the swing diesel, 13

If the offsite grid is available (top event OG in the support system event tree is successful) only the "G" events (GF, GG, GH) are questioned in the support systems event tree. If the offsite grid fails, all the five top events are questioned. The boundary conditions of these top events depend on the status of the preceding diesel generators in the event tree. Thus, top event GF has only one boundary condition (GF1) corresponding to the case when all support is available. GG has three boundary conditions (GG1, when GF succeeded; GG2, when GF failed; and GG3, when GF was bypassed, i.e., not demanded). Similarly GH has 6, 2G has 10, and 2H has 15 boundary conditions. Top event SW has four boundary conditions: one for LOCAs; one for LOOPs, when an equal number of diesels are operating at Unit 1 and Unit 2; and two for LOOPs, when an unequal number of diesels are operating at the two units.

Only one top event is defined in the DCPRA for the support system event tree associated with the diesel fuel oil transfer system . The designator of this top event is: LO. It is evaluated for six boundary conditions, depending

on the availability of 480V ac buses at both of the units (i.e., 1G, 2H, 2G, and 1H).

The success criteria of the above top events are described in Table 2.1. The Technical Specification requirements with respect to the operability of the associated systems are also indicated.

2.4 Logic Model of the Diesels and Diesel Fuel Oil Transfer System Dependency on Other Support Systems

The generic reliability block diagram for the diesel generators is shown in Figure 2.1. The diagram is constructed from blocks (supercomponents) of the DG system. The boundaries of the supercomponents (for instance: GH-1, GH-2A, GH-2B) are indicated in Figures 2.2 through 2.9. Notice, that the equipment boundaries for each of the diesels start with the diesel generator and include the output breaker, the fuel oil day tank, the day tank level control valves, and the undervoltage and transfer control relays. The diesel starting air system was not modelled separately because it was included as part of the diesel start failure data.

The reliability block diagram shows the dependencies on the super-components of the plant (ac and dc) electrical systems.

The reliability block diagram for the diesel fuel oil transfer system (Top Event, FO) is presented in Figure 2.10. The boundaries of the pump train blocks are indicated in Figure 2.11. The reliability block diagram shows also the system dependencies on other supercomponents of the plant (ac and dc) electrical systems.

2.5 Quantification of Top Event Split Fractions

The definitions of the boundary conditions and the associated split fractions for top events associated with the DG system are listed in Table

2.3. Table 2.4 presents a similar list for the diesel fuel oil transfer system (Top Event, LO).

Table 2.5 presents the values of diesel generator related top event split fraction values quantified by PG&E. Notice, that to provide better train-wise dependency tracking in the event tree model, the split fractions are expressed in terms of unavailabilities of various diesel state combinations (conditional split fractions, CSF). The arithmetic is explained in the DCPRA, Chapter D.2.1.5. The table presents also the total unavailability value (TTL) used in the calculation of each CSF, along with the main contributors to the total unavailabilities, such as hardware (HW), maintenance (MN), test (TS), and human error (HE). At a given boundary condition the hardware contribution relates to the normal alignment, when no test or maintenance activities are being performed. To provide complete information, the table also indicates the two constituent parts of the hardware contribution to the unavailability: the independent (HWI) and the dependent (HWD) (i.e., common cause) failures of the supercomponents of the diesels.

The maintenance contribution is a significant contributor to the total unavailability. The DCPRA assumes that, due to Technical Specification limitations, only one diesel or level control valve may be in maintenance at a time. The following relevant quantities are used in the maintenance unavailability quantification:

Diesel maintenance frequency, ZMDGSF: 7.74-4/hr (Mean Value). Variance = 2.33-8, 5th Percentile = 5.25-4, Median = 7.52-4, 95th Percentile = 9.66-4.

Diesel maintenance duration, ZMGSD: 1.01+1 hr (Mean Value). Variance = 3.99, 5th Percentile = 6.65, Median = 9.74, 95th Percentile = 13.3.

Level control valve maintenance frequency, ZMGNDF: 2.03-5/hr (Mean Value). Variance = 3.52-11, 5th Percentile = 1.14-5, Median = 1.91-5, 95th Percentile = 2.97-5.

Level control valve maintenance duration, ZMGN3D: 1.89+1 hr (Mean Value). Variance = 597.0, 5th Percentile = 1.54, Median = 10.1, 95th Percentile = 51.3.

Notice that the total maintenance unavailability of a diesel unit is determined by the diesel (as defined in DCPRA) maintenance unavailability plus the LCV maintenance unavailability. When a diesel is unavailable (not for reason of preventive maintenance) the other diesels must be surveillance tested once within 24 hours to verify operability. The DCPRA includes the unavailability contribution due to this type of test in the maintenance unavailability (MN).

The test contribution to the total unavailability is modelled in the DCPRA as to be due to the scheduled monthly surveillance tests, which include the manual test of the fuel transfer system to the diesels and the quarterly stroke test of the LCVs.

There is no explicit human error contribution to the total unavailability, because human errors occurring after maintenances and tests due to leaving diesel components in misalignment are included in the maintenance and test contributions.

Table 2.6 lists the split fraction values for the various boundary conditions of the FO top event. The table, as the previous one, details the hardware (independent and dependent components), maintenance test and human error contributions to the total unavailability values. Notice there are no explicit test or human error contributions. All the tests on fuel oil transfer system can be performed without making the system inoperable, human errors occurring leaving a fuel oil transfer train in misalignment after maintenance are included in unavailability values due to maintenance.

2.6 Quantification of Seismic Split Fractions for DG Top Events

The basis for detailing the seismic split fraction quantification for the DG top events is to provide insight into how the maintenance unavailability (and through it, the AOT) affects the seismic top events and consequently the seismic contribution to the core damage frequency. (This particular investigation was done as part of the parallel BNL DG AOT review as discussed in Section 1.)

All diesel generator components susceptible to failures by seismic events contribute to the diesel unavailability. The components considered to be the most vulnerable to seismic effects are the following:

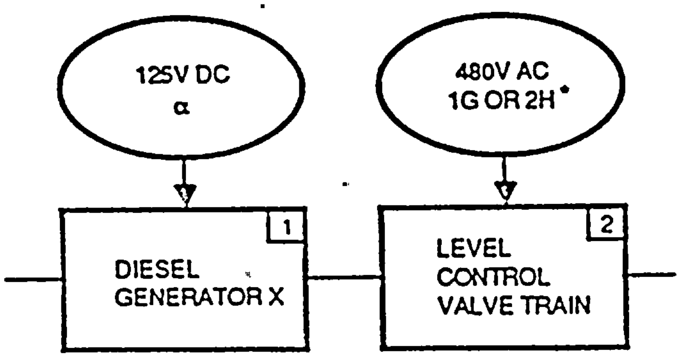
Component	Fragility Designator
DG Control Panel	ZDGCPN
DG Excitation Panel	ZDGEXC
DG Radiator/Water Pump	ZDGRWP
Diesel Generator Itself	ZDGSLGN

By using the conditional seismic failure probabilities ("fragilities"), the DCPRA combines them into a "seismic term" denoted by SEIST. SEIST has seven values corresponding to the seven seismic levels (i.e., spectral acceleration ranges) defined in the DCPRA. The seven SEIST values were determined by the mean fragilities of the diesel components listed in Table 6-44 on p.6-175 of Reference 1.

In order to calculate seismic split fractions, the DCPRA combines the SEIST values with the total unavailability values (TTL) coming from the conventional hardware, maintenance, test and human failures. In the case of seismic events, however, the DCPRA (correctly and innovatively) treats many human failures as seismic level-dependent; that is, the human factor probabilities are also dependent upon the seismic level.

To be more specific, the human failure which affects the TTL unavailabilities is the "failure to reestablish fuel oil transfer to day tanks by aligning a portable fuel oil transfer pump (see also Figure 2.10) and by controlling the day tank LCVs manually;" its designator is ZHEF06. For numerical values as a function of seismic level, see Appendix G of the DCPRA Table G.1-2, transmitted recently to BNL by PG&E.[4]

By using the resultant unavailabilities (SEIST + seismic level dependent TTL) the conditional seismic split fractions were determined for each diesel top events according to the rules of the sequential diesel failure model. These split fractions are listed as a function of the seismic level in Table 2.7. Each value of the table has a slight AOT dependence through the maintenance contribution to the TTL component of the unavailability.



X	α
13	11
12	12
11	13
21	22
22	23

DIESEL GENERATOR CONTROL POWER

* THESE ARE THE NORMAL POWER SUPPLIES FOR THE TWO LCV TRAINS; THE BACKUPS ARE 2G AND 1H RESPECTIVELY

Figure 2.1. Reliability block diagram for the diesel generators.

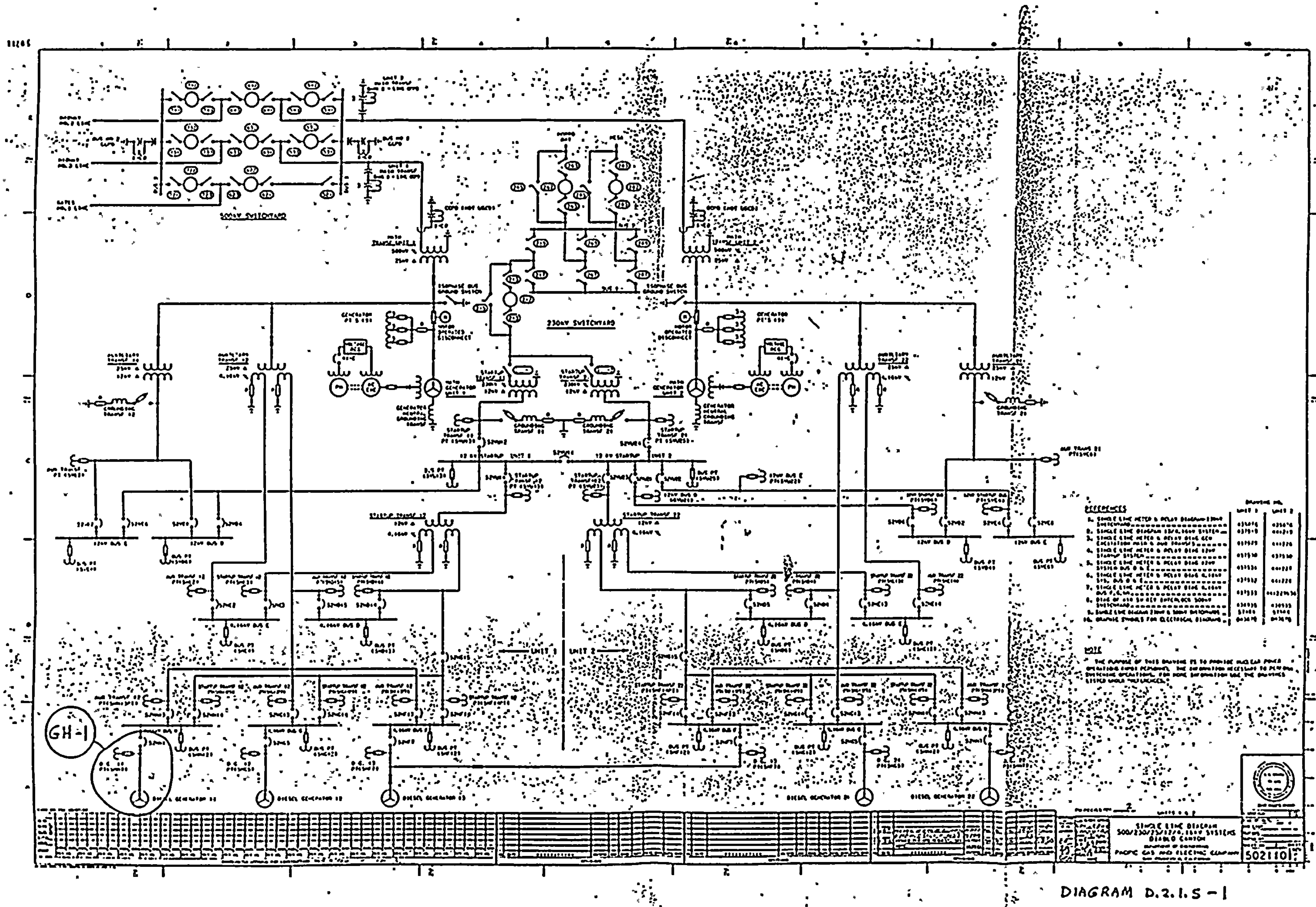


Figure 2.2. Diesel Generators; Supercomponents.

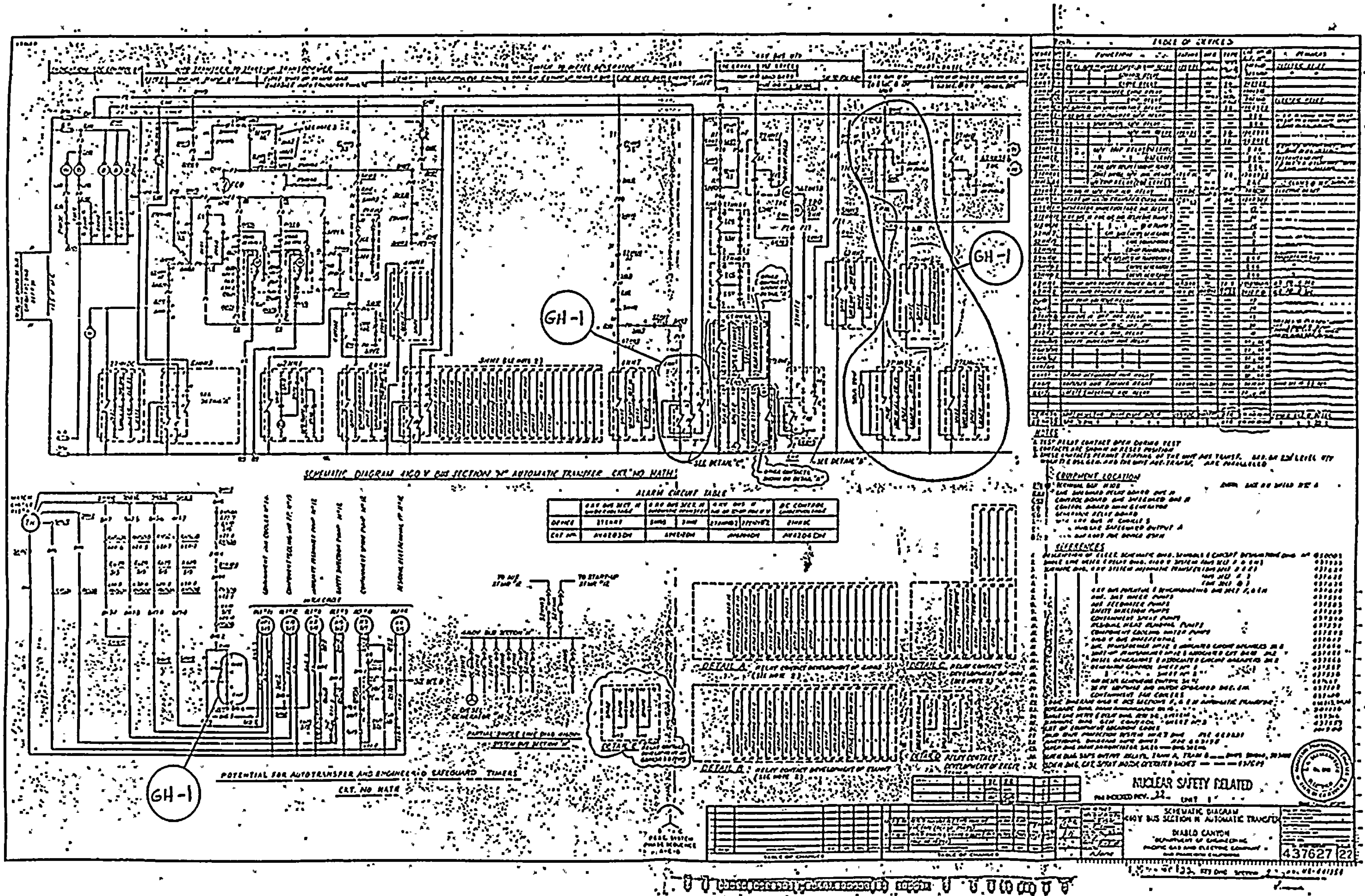


DIAGRAM D.2.1.S-2

Figure 2.3. Diesel Generators; Supercomponents.

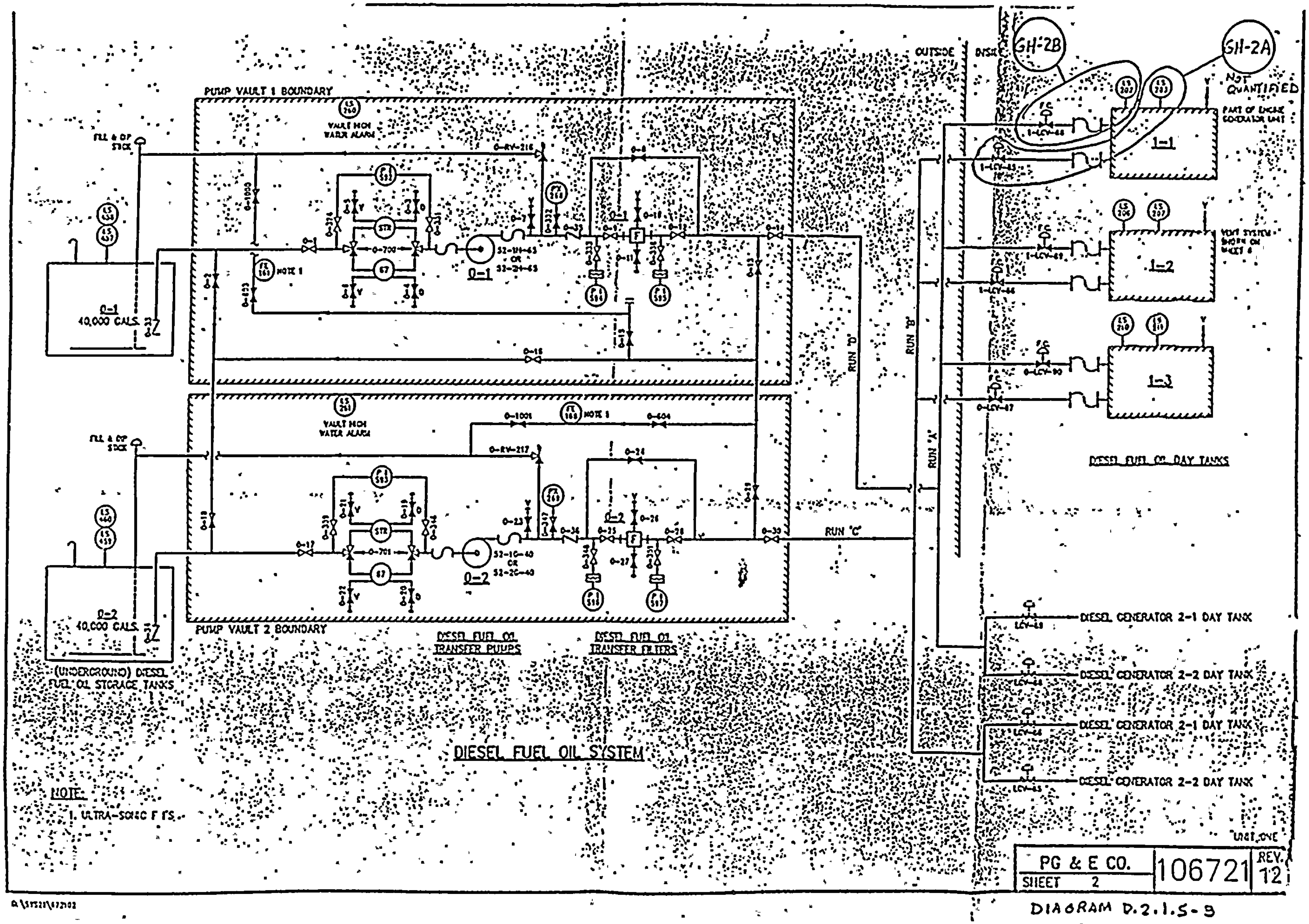


Figure 2.4. Diesel Generators; Supercomponents.

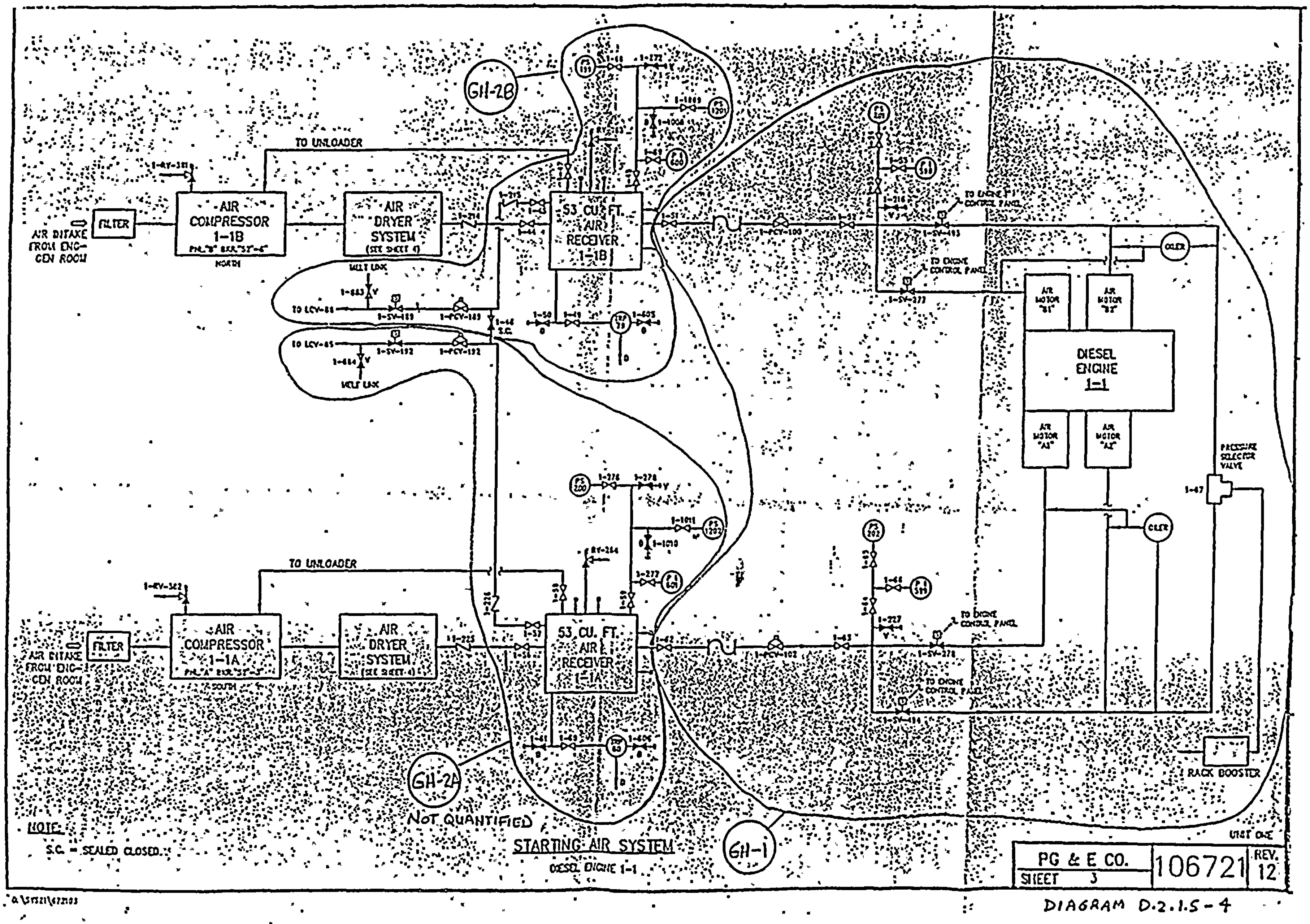


Figure 2.5. Diesel Generators; Supercomponents.

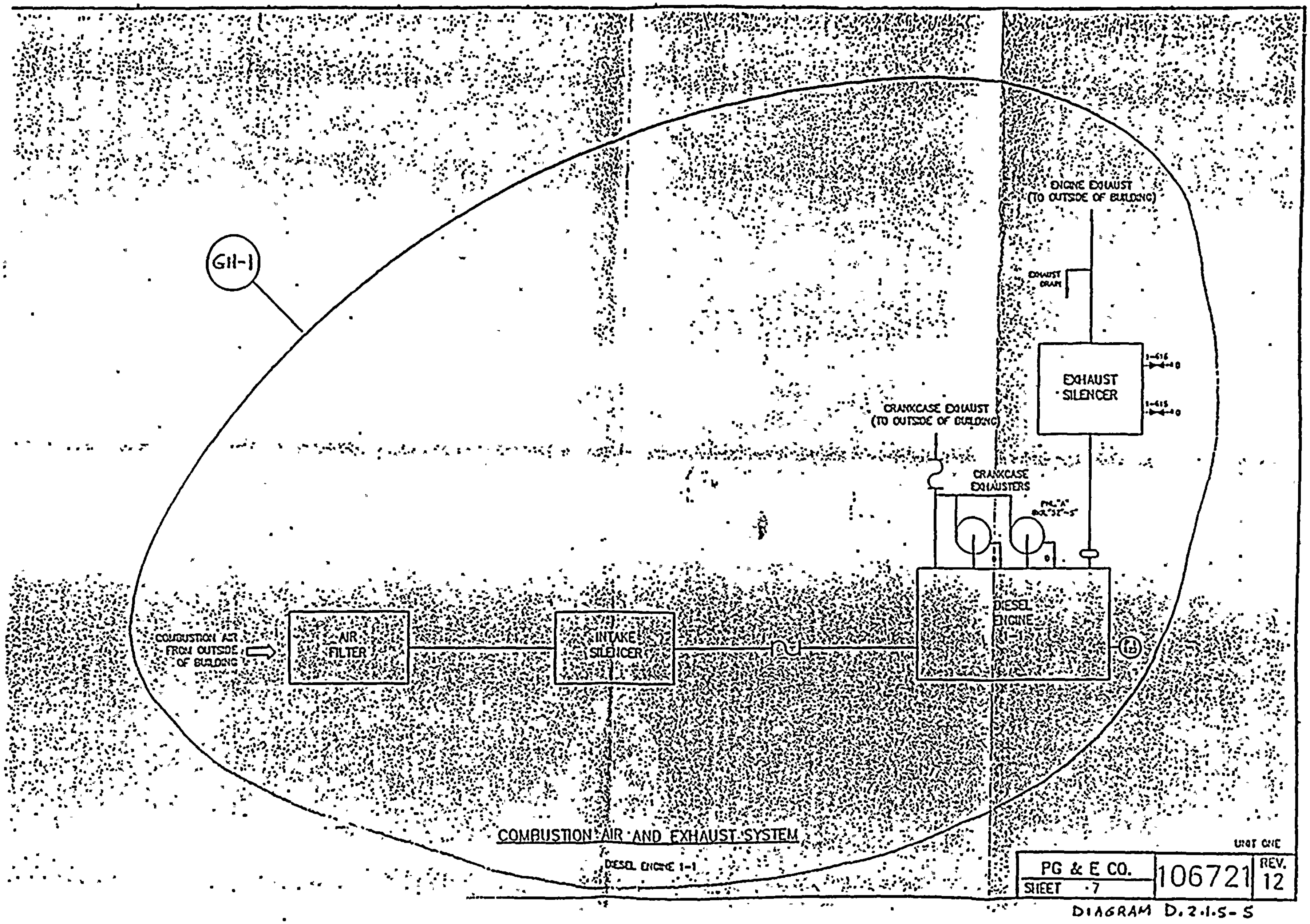
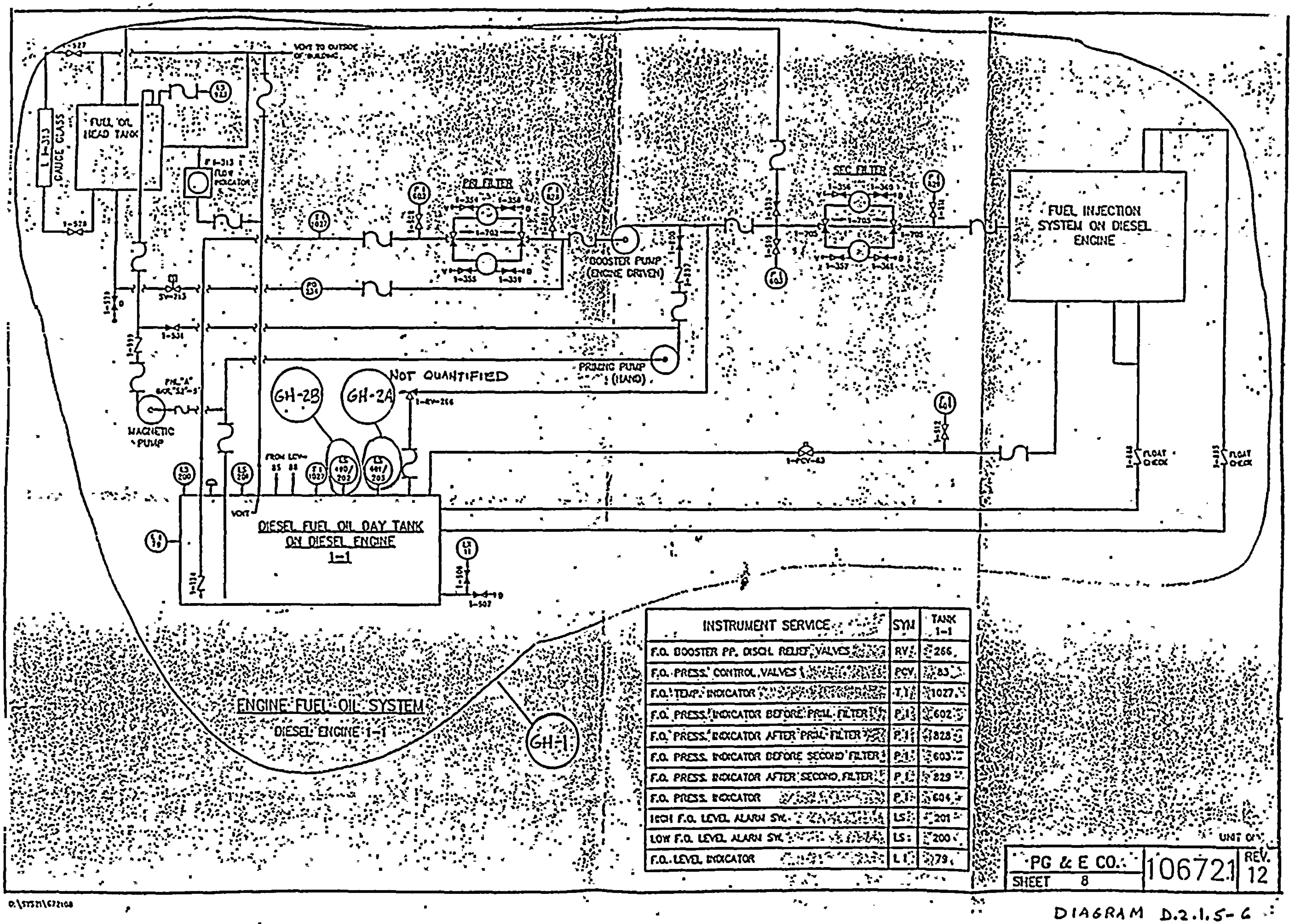


Figure 2.6. Diesel Generators; Supercomponents.



INSTRUMENT SERVICE	SYM	TANK 1-1
F.O. BOOSTER PP. DISCH. RELIEF VALVES	RV	266
F.O. PRESS. CONTROL VALVES	PCV	83
F.O. TEMP. INDICATOR	T.I.	1027
F.O. PRESS. INDICATOR BEFORE PRIM. FILTER	P.I.	602
F.O. PRESS. INDICATOR AFTER PRIM. FILTER	P.I.	828
F.O. PRESS. INDICATOR BEFORE SECOND FILTER	P.I.	603
F.O. PRESS. INDICATOR AFTER SECOND. FILTER	P.I.	829
F.O. PRESS. INDICATOR	P.I.	604
HIGH F.O. LEVEL ALARM SW.	LS	201
LOW F.O. LEVEL ALARM SW.	LS	200
F.O. LEVEL INDICATOR	L.I.	79

Figure 2.7. Diesel Generators; Supercomponents.

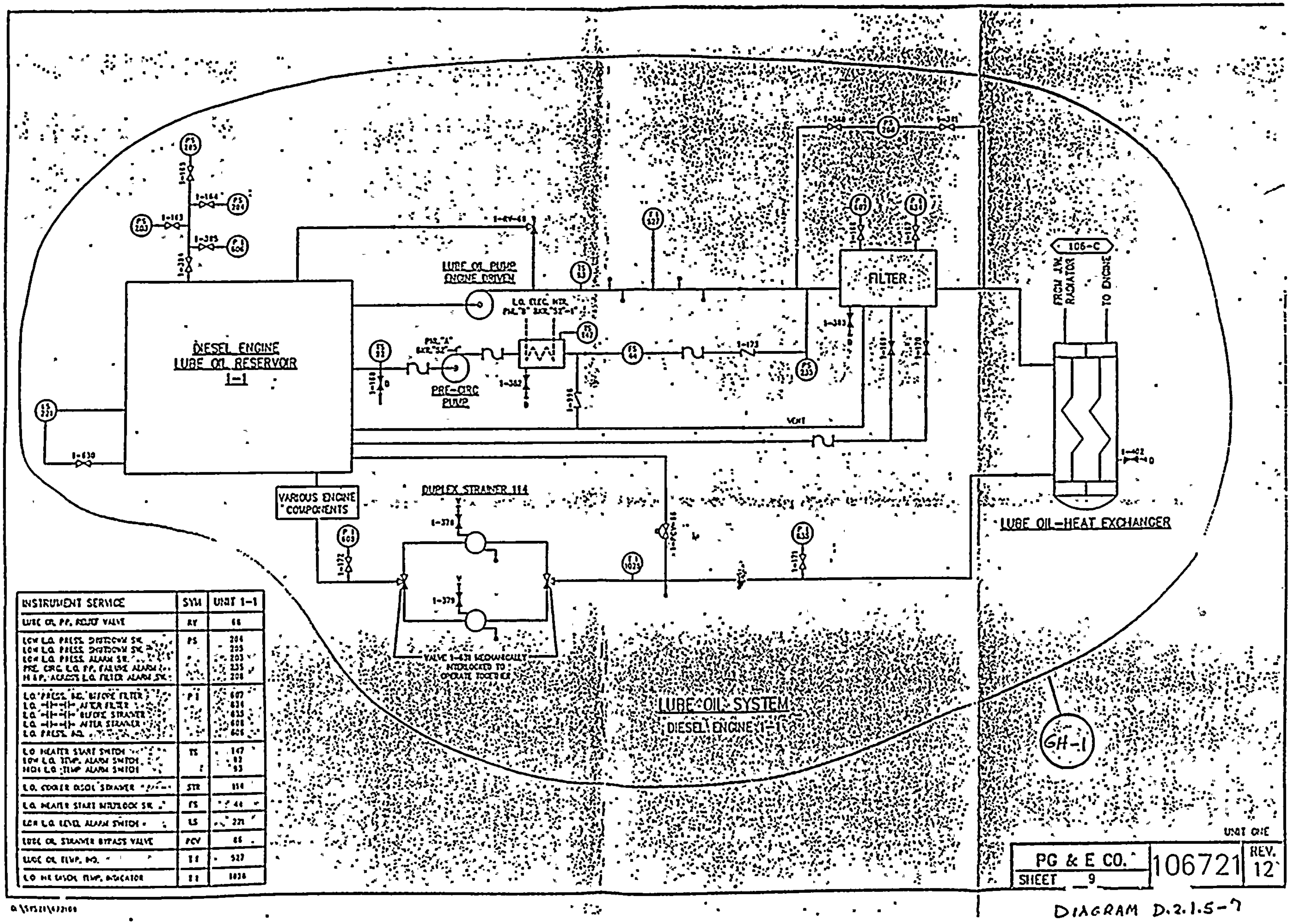


Figure 2.8. Diesel Generators; Supercomponents.

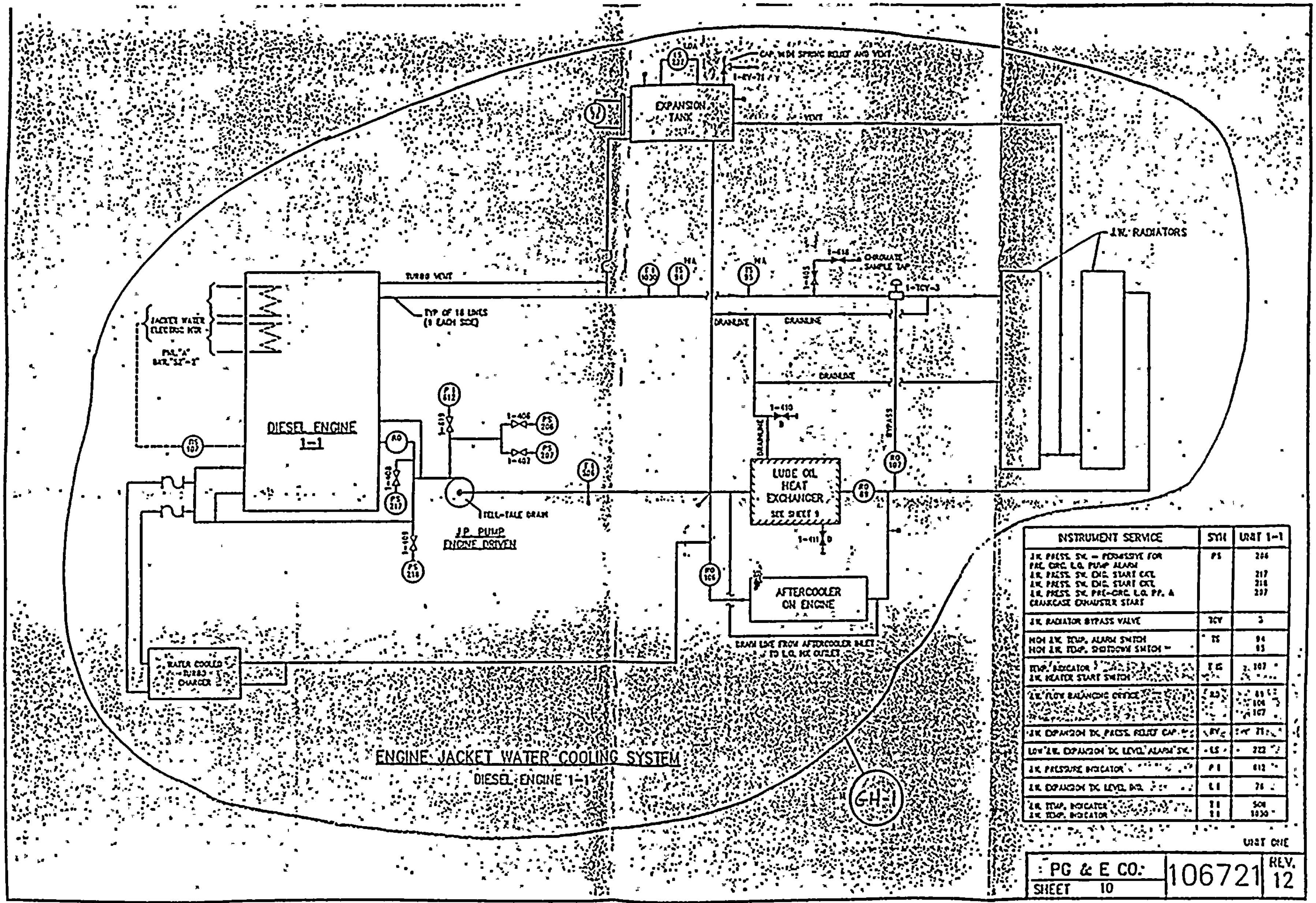
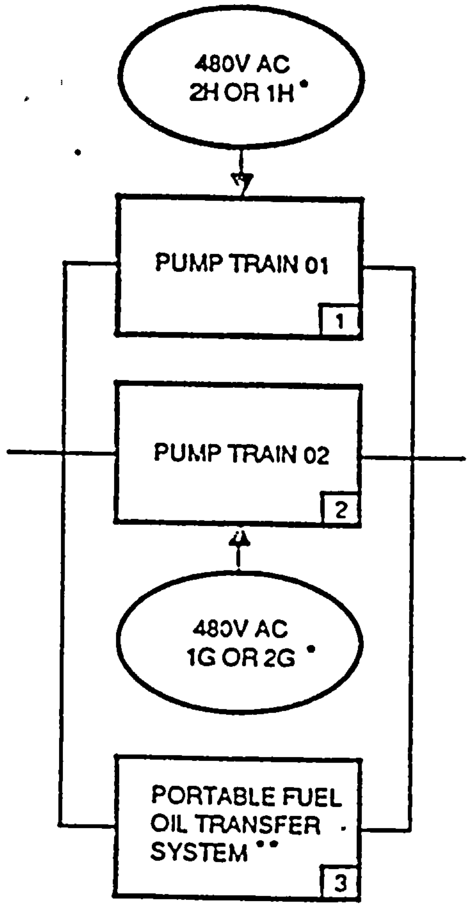


DIAGRAM D.2.1.5-8

Figure 2.9. Diesel Generators; Supercomponents.



* BACKUP POWER SOURCE
** THE PORTABLE FUEL OIL TRANSFER SYSTEM IS EVALUATED IN THE ELECTRIC POWER RECOVERY MODEL

Figure 2.10. Reliability block diagram for the diesel fuel oil transfer system (Top Event, FO).

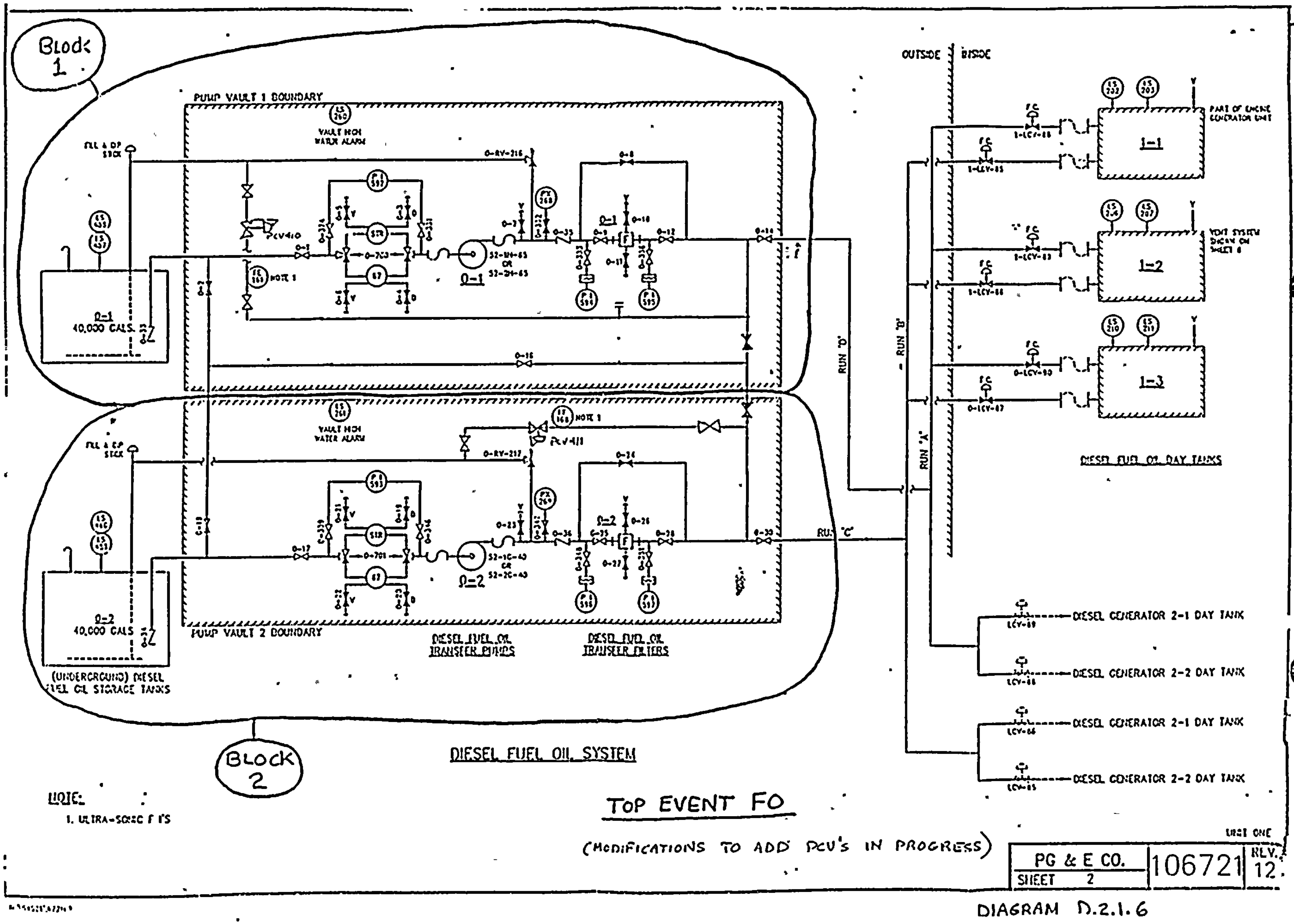


Figure 2.11. Top Event, FO - Supercomponents. Diesel fuel oil transfer system.

Table 2.1

Bus	DG	Vital Safety-Related Loads
F	1-3 (Swing)	Centrifugal Charging Pump No.1 Safety Injection Pump No.1 Containment Fan Cooler Unit No.2 Containment Fan Cooler Unit No.1 Component Cooling Water Pump No.1 Auxiliary Saltwater Pump No.1 Auxiliary Feedwater Pump No.3
G	1-2 (2-1)	Centrifugal Charging Pump No.2 Residual Heat Removal Pump No.1 Containment Fan Cooler Unit No.3 Containment Fan Cooler Unit No.5 Component Cooling Water Pump No.2 Auxiliary Saltwater Pump No.2 Containment Spray Pump No.1
H	1-1 (2-2)	Safety Injection Pump No.2 Residual Heat Removal Pump No.2 Containment Fan Cooler Unit No.4 Component Cooling Water Pump No.3 Auxiliary Feedwater Pump No.2 Containment Spray Pump No.2

Table 2.2
Top Event Definition and Success Criteria
Diesel Generator and Diesel Fuel Transfer Systems

Top Event Designator	Top Event Definition		Top Event Success Criteria
GF GG GH 2G 2H	DG13 provides power for DG12 6 hours (24 hours DG11 for seismic events) DG21 to 4.16kV ac buses DG22 (Bus index numbers indicate plant Unit No.)	$F_{1,2}$ G_1 H_1 G_2 H_2	Each top event is successful if the corresponding DG starts on undervoltage signal from its bus, takes bus loads and continues powering loads for the appropriate mission times (6 hours or 24 hours).
SW	Swing diesel alignment. DG13 is normally aligned to Unit 1.		The value of SW determines whether DG13 goes to Unit 2. A value of 0 indicates it does not, a value between 0 and 1 represents the probability that it does.
FO	Diesel fuel oil transfer system provides fuel oil for each of the DGs for six hours (24 hours for seismic events).		One of two pumps starts on low day tank level and refills each day tank for the period that each diesel operates.

FSAR Success Criteria:

Any two of three DGs and their associated buses are adequate to serve the vital loads necessary for safe shutdown of a single unit (although one DG may supply power to two vital buses at the same time, no credit is currently given this mode of operation).

The diesel fuel oil transfer system must remain operable and deliver fuel to each of the DGs for the time the DGs are required to operate. There must be enough fuel in storage tanks for seven days of power generation.

Technical Specifications:

With a single DG inoperable, demonstrate the operability of the remaining ac sources within 24 hours. Restore the diesel within 72 hours.

With two DGs inoperable, demonstrate the operability of the two offsite ac circuits (one 230kV and one 500kV line) within one hour and at least once every eight hours. Restore at least two of the inoperable diesels within two hours.

Table 2.3
Boundary Condition and Split Fraction Identifications
for Top Events GF, GG, GH, 2G, 2H, and SW

Top Event	Case	Diesel Conditions 13	12	11	21	22	Comments
GF - Unavailability of DG13 under the following conditions:							
	GF1						All support available.
GG - Unavailability of DG12 under the following conditions:							
	GG1	0					Offsite grid succeeded, GF succeeded.
	GG2	1					Offsite grid succeeded, GF failed.
	GG3	-					Offsite grid succeeded, GF bypassed (not demanded)
GH - Unavailability of DG11 under the following conditions:							
	GH1	0	0				Offsite grid succeeded, both GF, GG succeeded.
	GH2	0	1				Offsite grid succeeded, GF-S/F, GG-F/S (two possible combinations).
	GH3	1	1				Offsite grid succeeded, both GF, GG failed.
	GH4	0	-				Offsite grid succeeded, GF-S/B, GG-B/S (two possible combinations).
	GH5	1	-				Offsite grid succeeded, GF-F/B, GG-B/F (two possible combinations).
	GH6	-	-				Offsite grid succeeded, both GF, GG bypassed.
2G - Unavailability of DG21 under the following conditions:							
	2G1	0	0	0			Offsite grid failed, all GF, GG, and GH succeeded.
	2G2	0	0	1			Offsite grid failed, two of GF, GG, and GH succeeded, the third failed (three possible combinations).
	2G3	0	1	1			Offsite grid failed, two of GF, GG, GH failed, the third succeeded (three possible combinations).
	2G4	1	1	1			Offsite grid failed, all GF, GG, GH failed.
	2G5	0	0	-			Offsite grid failed, two of GF, GG, GH succeeded, the third bypassed (three possible combinations).

Table 2.3 (Continued)

Top Event	Case	Diesel Conditions 13	12	11	21	22	Comments
	2G6	0	1	-			Offsite grid failed, one of GF, GG, GH succeeded, one failed, the third bypassed (six possible combinations).
	2G7	1	1	-			Offsite grid failed, two of GF, GG, GH failed, the third bypassed (three possible combinations).
	2G8	0	-	-			Offsite grid failed, one of GF, GG, GH succeeded, the other two bypassed (three possible combinations).
	2G9	1	-	-			Offsite grid failed, one of GF, GG, GH failed, the other two bypassed (three possible combinations).2GA---Offsite grid failed, all of GF, GG, GH bypassed.
2H - Unavailability of DG22 under the following conditions:							
	2H1	0	0	0	0		Offsite grid failed, all of GF, GG, GH, 2G succeeded.
	2H2	1	0	0	0		Offsite grid failed, one of GF, GG, GH, 2G failed, the other three succeeded (four possible combinations).
	2H3	1	1	0	0		Offsite grid failed, two of GF, GG, GH, 2G failed, the other two succeeded (six possible combinations).
	2H4	1	1	1	0		Offsite grid failed, three of GF, GG, GH, 2G failed, the fourth succeeded (four possible combinations).
	2H5	1	1	1	1		Offsite grid failed, all of GF, GG, GH, 2G failed.
	2H6	0	0	0	-		Offsite grid failed, three of GF, GG, GH, 2G succeeded, the fourth bypassed (four possible combinations).
	2H7	0	0	1	-		Offsite grid failed, two of GF, GG, GH, 2G succeeded, one failed, the fourth bypassed (12 possible combinations).
	2H8	0	1	1	-		Offsite grid failed, two of GF, GG, GH, 2G failed, one succeeded, the

Table 2.3 (Continued)

Top Event	Case	Diesel Conditions 13	12	11	21	22	Comments
							fourth bypassed (12 possible combinations).
	2H9	1	1	1	-		Offsite grid failed, three of GF, GG, GH, 2G failed, the fourth bypassed (four possible combinations).
	2HA	0	0	-	-		Offsite grid failed, two of GF, GG, GH, 2G succeeded, the other two bypassed (six possible combinations).
	2HB	-	-	1	0		Offsite grid failed, two of GF, GG, GH, 2G bypassed, one failed, the fourth succeeded (12 possible combinations).
	2HC	-	-	1	1		Offsite grid failed, two of GF, GG, GH, 2G bypassed, the other two failed (six possible combinations).
	2HD	-	-	-	0		Offsite grid failed, three of GF, GG, GH, 2G bypassed, the fourth succeeded (four possible combinations).
	2HE	-	-	-	1		Offsite grid failed, three of GF, GG, GH, 2G bypassed, the fourth failed (four possible combinations).
	2HG	-	-	-	-		Offsite grid failed, all of GF, GG, GH, 2G bypassed.
SW	SW0						LOCA, the swing diesel locked to the Unit 1.
	SW1						LOSP, with equal chance for swing diesel to operate on each unit.
	SW2						LOSP, with more DGs aligned to Unit 2 than Unit 1.
	SW3						LOSP, with more DGs aligned to Unit 1 than Unit 2.

Notes: 0 = Succeeded
1 = Failed
\- = Bypassed

Table 2.4
Diesel Fuel Oil Transfer System Boundary
Conditions for Top Event, LO

Split Fraction ID	
F01	All support available.
F02	Support available to one train only.
F03	1/2 normal support available; recover support to the other train by realignment to backup support.
F04	2/2 normal support unavailable; recover supports by realignment to backups.
F05	2/2 normal supports unavailable; recover only 1/2 backup support by realignment.
F06	All support unavailable (guaranteed failure).

Table 2.5
Unavailability Values (Conditional Split Fractions) for the
Diesel Generator System

Top Event	Case	Calc.	CSF	TTL	HW	HWI	HWD	TS	MN	HE	Comment #
GF	GF1	PG&E	4.523-2	4.554-2	3.703-2	3.689-2	1.393-4	2.950-4	8.217-3	--	
		BNL	4.571-2	4.603-2	3.754-2	3.695-2	5.860-4	2.934-4	8.198-3		
GG	GG1	PG&E	4.477-2	4.554-2	as GF1						
		BNL	4.527-2	4.603-2							
	GG2	PG&E	5.561-2	2.702-3	1.749-3	1.536-3	2.129-4	4.989-5	9.025-4	--	
		BNL	5.474-2	2.540-3	1.581-3	1.366-3	2.149-4	4.980-5	9.089-4	--	
	GG3	PG&E	4.523-2	4.554-2	as GF1						
		BNL	4.571-2	4.603-2							
GH	GH1	PG&E	4.436-2	4.554-2	as GF1						
		BNL	4.490-2	4.603-2							
	GH2	PG&E	5.408-2	2.702-3	as GG2						
		BNL	5.322-2	2.540-3							
	GH3	PG&E	8.265-2	2.339-4	1.264-4	7.438-5	5.204-5	3.173-5	7.566-5	--	
		BNL	8.097-2	2.066-4	1.034-4	5.057-5	5.284-5	3.128-5	7.194-5	--	
	GH4	PG&E	4.477-2	4.554-2	as GF1						
		BNL	4.527-2	4.603-2							
	GH5	PG&E	5.561-2	2.702-3	as GG2						
		BNL	5.474-2	2.540-3							
	GH6	PG&E	4.523-2	4.554-2	as GF1						
		BNL	4.571-2	4.603-2							
2G	2G1	PG&E	4.396-2	4.554-2	as GF1						
		BNL	4.453-2	4.603-2							
	2G2	PG&E	5.364-2	2.702-3	as GG2						
		BNL	5.271-2	2.540-3							
	2G3	PG&E	6.250-2	2.339-4	as GH3						
		BNL	6.246-2	2.066-4							
	2G4	PG&E	2.898-1	6.369-5	2.597-5	4.314-6	2.166-5	3.049-5	7.221-6	--	
		BNL	2.910-1	5.995-5	2.363-5	1.874-6	2.176-5	3.017-5	6.176-6	--	

Table 2.5 (Continued)

Top Event	Case	Calc.	CSF	TTL	HW	HWI	HWD	TS	MN	HE	Comment #
	2HA	PG&E	4.436-2	4.554-2	as GF1						
		BNL	4.490-2	4.603-2							
	2HB	PG&E	5.408-2	2.702-3	as GG2						
		BNL	5.322-2	2.540-3							
	2HC	PG&E	8.265-2	2.339-4	as GH3						
		BNL	8.098-2	2.066-4							
	2HD	PG&E	4.477-2	4.554-2	as GF1						
		BNL	4.527-2	4.603-2							
	2HE	PG&E	5.561-2	2.702-3	as GG2						
		BNL	5.474-2	2.540-3							
	2HG	PG&E	4.523-2	4.554-2	as GF1						
		BNL	4.571-2	4.603-2							
SW	SW0	PG&E		0.000							
		BNL		0.000							
	SW1	PG&E		5.000-1							
		BNL		5.000-1							
	SW2	PG&E		1.767-3							
		BNL		1.770-3							
	SW3	PG&E		9.981-1							
		BNL		9.982-1							

Table 2.6
Unavailability Values (Split Fractions) for the
Diesel Fuel Transfer System

Top Event	Case	Calc.	TTL	HW	HWI	HWD	TS	MN	HE
FO	F01	PG&E	2.164-4	1.919-4	1.176-5	1.802-4	0.0	2.445-5	0.0
		BNL	2.092-4	1.848-4	8.533-6	1.763-4	0.0	2.447-5	0.0
	F02	PG&E	7.040-3	3.113-3	2.933-3	1.802-4	0.0	3.930-3	0.0
		BNL	7.048-3	3.097-3	2.921-3	1.763-4	0.0	3.951-3	0.0
	F03	PG&E	3.509-4	1.919-4	1.176-5	1.802-4	0.0	2.445-5	0.0
		BNL	3.460-4	1.848-4	8.533-6	1.763-4	0.0	2.447-5	0.0
	F04	PG&E	2.263-2	1.919-4	1.176-5	1.802-4	0.0	2.445-5	0.0224
		BNL	2.250-2	1.848-4	8.533-6	1.763-4	0.0	2.447-5	0.0223
	F05	PG&E	5.079-2	3.113-3	2.933-3	1.802-4	0.0	3.930-3	0.0224
		BNL	2.292-2	3.097-3	2.921-3	1.763-4	0.0	3.951-3	0.0223
	FOF	PG&E	1.0						
		BNL	1.0						

Table 2.7a
Conditional Split Fractions for DG Top Events
as a Function of Seismic Level

PG&E

Split Fraction ID	Seismic Level (spectral acceleration, g) 0.0-0.2	0.2-1.25	1.25-1.75	1.75-2.0	2.0-2.5	2.5-3.0	3.0-4.0
CT1	8.5100E-02	8.5100E-02	8.5660E-02	9.3020E-02	1.0550E-01	1.7000E-01	2.8270E-01
CG1	8.4170E-02	8.4170E-02	8.4170E-02	8.7670E-02	8.7670E-02	1.0560E-01	1.0560E-01
CG2	9.5020E-02	9.5020E-02	1.0150E-01	1.4510E-01	2.5700E-01	4.8460E-01	7.3210E-01
CG3	8.5100E-02	8.5100E-02	8.5660E-02	9.3020E-02	1.0550E-01	1.7000E-01	2.8270E-01
CH1	8.3340E-02	8.3340E-02	8.3340E-02	8.6700E-02	8.6700E-02	1.0430E-01	1.0430E-01
CH2	9.3290E-02	9.3290E-02	9.3290E-02	9.7810E-02	9.7810E-02	1.1630E-01	1.1630E-01
CH3	1.1150E-01	1.1150E-01	1.7450E-01	4.2380E-01	7.1720E-01	8.7630E-01	9.5750E-01
CH4	8.4170E-02	8.4170E-02	8.4170E-02	8.7670E-02	8.7670E-02	1.0560E-01	1.0560E-01
CH5	9.5020E-02	9.5020E-02	1.0150E-01	1.4510E-01	2.5700E-01	4.8460E-01	7.3210E-01
CH6	8.5100E-02	8.5100E-02	8.5660E-02	9.3020E-02	1.0550E-01	1.7000E-01	2.8270E-01
2G1	8.2510E-02	8.2510E-02	8.2510E-02	8.5740E-02	8.5740E-02	1.0310E-01	1.0310E-01
2G2	9.2440E-02	9.2440E-02	9.2440E-02	9.6770E-02	9.6770E-02	1.1490E-01	1.1490E-01
2G3	1.0160E-01	1.0160E-01	1.0160E-01	1.0740E-01	1.0740E-01	1.2650E-01	1.2650E-01
2G4	1.9030E-01	1.9030E-01	5.1950E-01	8.5400E-01	9.5770E-01	9.8210E-01	9.9440E-01
2G5	8.3340E-02	8.3340E-02	8.3340E-02	8.6700E-02	8.6700E-02	1.0430E-01	1.0430E-01
2G6	9.3290E-02	9.3290E-02	9.3290E-02	9.7810E-02	9.7810E-02	1.1630E-01	1.1630E-01
2G7	1.1150E-01	1.1150E-01	1.7450E-01	4.2380E-01	7.1720E-01	8.7630E-01	9.5750E-01
2G8	8.4170E-02	8.4170E-02	8.4170E-02	8.7670E-02	8.7670E-02	1.0560E-01	1.0560E-01
2G9	9.5020E-02	9.5020E-02	1.0150E-01	1.4510E-01	2.5700E-01	4.8460E-01	7.3210E-01
2GA	8.5100E-02	8.5100E-02	8.5660E-02	9.3020E-02	1.0550E-01	1.7000E-01	2.8270E-01
2H1	8.1690E-02	8.1690E-02	8.1690E-02	8.4800E-02	8.4800E-02	1.0190E-01	1.0190E-01
2H2	9.1620E-02	9.1620E-02	9.1620E-02	9.5780E-02	9.5780E-02	1.1360E-01	1.1360E-01
2H3	1.0050E-01	1.0050E-01	1.0050E-01	1.0600E-01	1.0600E-01	1.2470E-01	1.2470E-01
2H4	1.1120E-01	1.1120E-01	1.1120E-01	1.1890E-01	1.1890E-01	1.3930E-01	1.3930E-01
2H5	5.2690E-01	5.2690E-01	8.9720E-01	9.7970E-01	9.9470E-01	9.9750E-01	9.9920E-01
2H6	8.2510E-02	8.2510E-02	8.2510E-02	8.5740E-02	8.5740E-02	1.0310E-01	1.0310E-01
2H7	9.2440E-02	9.2440E-02	9.2440E-02	9.6770E-02	9.6770E-02	1.1490E-01	1.1490E-01
2H8	1.0160E-01	1.0160E-01	1.0160E-01	1.0740E-01	1.0740E-01	1.2650E-01	1.2650E-01
2H9	1.9030E-01	1.9030E-01	5.1950E-01	8.5400E-01	9.5770E-01	9.8210E-01	9.9440E-01
2HA	8.3340E-02	8.3340E-02	8.3340E-02	8.6700E-02	8.6700E-02	1.0430E-01	1.0430E-01
2HB	9.3290E-02	9.3290E-02	9.3290E-02	9.7810E-02	9.7810E-02	1.1630E-01	1.1630E-01
2HC	1.1150E-01	1.1150E-01	1.7450E-01	4.2380E-01	7.1720E-01	8.7630E-01	9.5750E-01
2HD	8.4170E-02	8.4170E-02	8.4170E-02	8.7670E-02	8.7670E-02	1.0560E-01	1.0560E-01
2HE	9.5020E-02	9.5020E-02	1.0150E-01	1.4510E-01	2.5700E-01	4.8460E-01	7.3210E-01
2HG	8.5100E-02	8.5100E-02	8.5660E-02	9.3020E-02	1.0550E-01	1.7000E-01	2.8270E-01
SW0	0.0000E-01	0.0000E-01	0.0000E-01	0.0000E-01	0.0000E-01	0.0000E-01	0.0000E-01
SW1	5.0000E-01	5.0000E-01	5.0000E-01	5.0000E-01	5.0000E-01	5.0000E-01	5.0000E-01
SW2	1.7500E-03	1.7500E-03	1.7500E-03	1.0000E-02	1.0000E-02	5.0000E-02	5.0000E-02
SW3	9.9820E-01	9.9820E-01	9.9820E-01	9.9000E-01	9.9000E-01	9.5000E-01	9.5000E-01

Table 2.7b
Conditional Split Fractions for DG Top Events
as a Function Seismic Level

BNL

Split Fraction ID	Seismic Level (spectral acceleration, g) 0.0-0.2	0.2-1.25	1.25-1.75	1.75-2.0	2.0-2.5	2.5-3.0	3.0-4.0
GF1=	8.389E-02	8.389E-02	8.445E-02	9.193E-02	1.044E-01	1.694E-01	2.815E-01
GG1=	8.325E-02	8.325E-02	8.325E-02	8.687E-02	8.687E-02	1.054E-01	1.054E-01
GG2=	9.085E-02	9.087E-02	9.748E-02	1.419E-01	2.551E-01	4.831E-01	7.309E-01
GG3=	8.389E-02	8.389E-02	8.445E-02	9.193E-02	1.044E-01	1.694E-01	2.815E-01
GH1=	8.272E-02	8.272E-02	8.272E-02	8.618E-02	8.618E-02	1.044E-01	1.044E-01
GH2=	8.913E-02	8.913E-02	8.913E-02	9.417E-02	9.417E-02	1.145E-01	1.145E-01
GH3=	1.080E-01	1.082E-01	1.747E-01	4.306E-01	7.250E-01	8.774E-01	9.578E-01
GH4=	8.325E-02	8.325E-02	8.325E-02	8.687E-02	8.687E-02	1.054E-01	1.054E-01
GH5=	9.085E-02	9.087E-02	9.748E-02	1.419E-01	2.551E-01	4.831E-01	7.309E-01
GH6=	8.389E-02	8.389E-02	8.445E-02	9.193E-02	1.044E-01	1.694E-01	2.815E-01
2G1=	8.221E-02	8.221E-02	8.221E-02	8.553E-02	8.553E-02	1.034E-01	1.034E-01
2G2=	8.827E-02	8.827E-02	8.827E-02	9.306E-02	9.306E-02	1.130E-01	1.130E-01
2G3=	9.794E-02	9.794E-02	9.794E-02	1.048E-01	1.048E-01	1.264E-01	1.264E-01
2G4=	1.908E-01	1.929E-01	5.374E-01	8.614E-01	9.603E-01	9.823E-01	9.944E-01
2G5=	8.272E-02	8.272E-02	8.272E-02	8.618E-02	8.618E-02	1.044E-01	1.044E-01
2G6=	8.913E-02	8.913E-02	8.913E-02	9.417E-02	9.417E-02	1.145E-01	1.145E-01
2G7=	1.080E-01	1.082E-01	1.747E-01	4.306E-01	7.250E-01	8.774E-01	9.578E-01
2G8=	8.325E-02	8.325E-02	8.325E-02	8.687E-02	8.687E-02	1.054E-01	1.054E-01
2G9=	9.085E-02	9.087E-02	9.748E-02	1.419E-01	2.551E-01	4.831E-01	7.309E-01
2GA=	8.389E-02	8.389E-02	8.445E-02	9.193E-02	1.044E-01	1.694E-01	2.815E-01
2H1=	8.175E-02	8.175E-02	8.175E-02	8.492E-02	8.492E-02	1.024E-01	1.024E-01
2H2=	8.744E-02	8.744E-02	8.744E-02	9.200E-02	9.200E-02	1.115E-01	1.115E-01
2H3=	9.688E-02	9.688E-02	9.688E-02	1.034E-01	1.034E-01	1.246E-01	1.246E-01
2HA=	1.077E-01	1.077E-01	1.077E-01	1.166E-01	1.166E-01	1.382E-01	1.382E-01
2H5=	5.433E-01	5.495E-01	9.073E-01	9.812E-01	9.952E-01	9.975E-01	9.992E-01
2H6=	8.221E-02	8.221E-02	8.221E-02	8.553E-02	8.553E-02	1.034E-01	1.034E-01
2H7=	8.827E-02	8.827E-02	8.827E-02	9.306E-02	9.306E-02	1.130E-01	1.130E-01
2H8=	9.794E-02	9.794E-02	9.794E-02	1.048E-01	1.048E-01	1.264E-01	1.264E-01
2H9=	1.908E-01	1.929E-01	5.374E-01	8.614E-01	9.603E-01	9.823E-01	9.944E-01
2HA=	8.272E-02	8.272E-02	8.272E-02	8.618E-02	8.618E-02	1.044E-01	1.044E-01
2HB=	8.913E-02	8.913E-02	8.913E-02	9.417E-02	9.417E-02	1.145E-01	1.145E-01
2HC=	1.080E-01	1.082E-01	1.747E-01	4.306E-01	7.250E-01	8.774E-01	9.578E-01
2HD=	8.325E-02	8.325E-02	8.325E-02	8.687E-02	8.687E-02	1.054E-01	1.054E-01
2HE=	9.085E-02	9.087E-02	9.748E-02	1.419E-01	2.551E-01	4.831E-01	7.309E-01
2HG=	8.389E-02	8.389E-02	8.445E-02	9.193E-02	1.044E-01	1.694E-01	2.815E-01
SW0=	0.000E-01	0.000E-01	0.000E-01	0.000E-01	0.000E-01	0.000E-01	0.000E-01
SW1=	5.000E-01	5.000E-01	5.000E-01	5.000E-01	5.000E-01	5.000E-01	5.000E-01
SW2=	1.770E-03	1.770E-03	1.770E-03	1.000E-02	1.000E-02	5.000E-02	5.000E-02
SW3=	9.982E-01	9.982E-01	9.982E-01	9.900E-01	9.900E-01	9.500E-01	9.500E-01

3. RESULTS OF THE BNL REVIEW

3.1 General

The unavailability modelling of the Diesel Generators and the Diesel Fuel Transfer System in the DCPRA were reviewed by BNL with special emphasis because of the following:

a. The DGs are the most important support systems; impacting the safety of the majority of plant operations, including cold shutdown.
b. As discussed in Section 1, a request for changing the Allowed Outage Time (AOT) of the Diesel Generators was submitted to the NRC by PG&E and the study[2] supporting the request is based mainly on the DCPRA. BNL is reviewing this study in a parallel effort to this review.

Therefore, to check the adequacy of the DCPRA modelling for "system-specific" effects which may also influence granting permission for AOT changes, BNL used the following approach: BNL compared the vendor-specific (ALCO) diesel failure events with those obtained from generic diesel data. This was done to see how well the DCPRA model reflects the vendor-specific "experience" and to estimate the expected downtime distribution of the diesels. The evaluation was carried out by reviewing the failure modes and maintenance unavailabilities involved in the diesel model. In order to check for calculational inconsistencies, all of the split fractions were recalculated (seismic inclusive).

3.2 Comparison of ALCO Type DG Failures With All Types of DG Failures

In order to see whether the ALCO-type DGs used at the Diablo Canyon power plant have some subsystem- or component-specific failure modes (and thus, some subsystem or component specific expected downtimes) BNL compared the leading failure contributions of subsystems and components of ALCO diesels with those of all other types of DGs. The data were taken from a recent study performed at Battelle on aging of diesel components.[5] Table 3.1 presents the results.

One can see that the Instruments and Control System's (and within it the governor's) failures are the main contributors to the generic failures of ALCO diesels. Also with ALCO diesels, the Cooling System and to a lesser extent the Lubrication System seem to be more prone to failures than in the total generic DG population. A positive feature of the ALCO diesels is that the starting system appears to be less vulnerable to failure than the generic DG population. Finally, the ALCO fuel system does not seem to be any more prone to failures than the generic one.

3.3 Remarks on the Unavailability Modelling of the Diesels and Fuel Oil Transfer System in the DCPRA

a. The system modelling of the DGs in the DCPRA represents an elaborate sequential unavailability analysis of a "five train" system, where one train (the swing diesel) is playing a special role. There is no question that the approach used is mathematically appealing because it uses the symmetry aspects of the diesel configuration and renders the results of the analysis very suitable for integration into the DCPRA. The complexity of the calculation, however, for casual readers is difficult and for eventual uses (e.g., change of AOT) is rather cumbersome.

b. In contrast with the systems modelling, the unavailability modelling of the individual diesels (the fault tree modelling) was kept simplistic by using the standard "diesel fails to start and run" failure modes. The diesel starting air system (i.e., air compressors, receivers, etc.) were not modelled separately because they were considered to be included as part of the diesel start failure data. An attempt was made to display some components of the diesel subsystems in the model. This effort, however, tended to be inconsistent in that only some support failures were modelled and inconsequential in that the modelled failures were of such low probability. For example, each supercomponent "2A" and "2B" contains the failure rates: "DG Air Receiver - Rupture During Operation: ZTTK1B - 2.66-8/hr," "Air Check Valve - Transfer Closed During Operation: ZTVCOP - 1.04-

8/hr," etc. The failure contribution of the turbocharger, however, with an estimated[2] failure probability of 2.73-4/d was neglected.

Another example: while the diesel supercomponent boundaries indicate several subsystems as part of the supercomponents (see Figures 2.6, 2.8, and 2.9), one cannot find any representative component failure rate contributing to the combined unavailability of those supercomponents. Such subsystems are: the cooling, the lubrication and the combustion air systems. Table 3.1 shows that the cooling system is the second largest contributor to the failure of the ALCO type diesels.

c. The following remark also has relevance in connection with the AOT study[2] and concerns the expected downtime distribution of the diesel systems. The DCPRA models the maintenance frequency and duration of the LCVs as separate quantities from those of the diesels. If the day tank and other fuel system components are included in the maintenance data of the diesel, it is not clear why the LCV is treated separately. Given that it is treated separately, the mean and 95th percentile of the "effective" downtime distribution of the diesel system would be determined by the combination of the diesel and the LCV maintenance duration distributions (the 95th percentile value of the LCV maintenance durations is 51.3 hours).

d. The DCPRA considers only unscheduled maintenances performed on Unit 2 diesels as contributing to the unavailabilities of the associated top events, "2G" and "2H." Unavailabilities due to large overhauls lasting over a protracted period of time performed when Unit 1 is operating and Unit 2 is in refueling (or cold shutdown) (say two times 10 to 16 days each) were not included in the model.

e. In Table 2.6 the PG&E total split fraction value, FO5 seems to be in variance with that obtained by BNL. The probable cause of the discrepancy is that the human error contribution was double counted in the DCPRA. The PG&E value is seemingly also in contradiction with the PG&E seismic values

given at the lowest three seismic levels in Table 6-46 (p.6-182) of Reference 1.

f. The detailed analysis of the Fuel Oil Transfer System (see Figure D.2.1-3 Sheet 3 of 4) contains the following item (Item No.12): "In an emergency where it is necessary to get into the fuel oil pump vault to manipulate valves, it may take several hours to get security to open the vault." This item renders questionable the estimates of the human factors (among others the value of ZHEF06 used in the diesel analysis) considered for recovery of the Fuel Oil Transfer System and through it, the recovery of electrical power.

g. Among the DG failure related LERs filed by the Diablo Canyon power plant,[6] there was one failure in the Fuel Oil Transfer System which would affect all the DGs. This common cause failure involved the degradation of the diesel oil in the underground reserve tanks caused by fungi. According to PG&E, the problem does not exist any more. However because of its peculiarity and importance it is quoted here:

> LER 88-14. This report is being voluntarily submitted for information purposes only as described in Item 19 of Supplement No.1 to NUREG-1022. On May 4, 1988, during performance of surveillance test procedure (SRP) M-96, "diesel generator 24 hour load test," the diesel generator (DG) 1-1 load decreased below the value specified in the SRP acceptance criteria. An investigation showed that a high differential pressure existed across the primary fuel oil filter. After switching to the standby primary fuel oil filter, the load returned to the required value. An investigation determined that the DG day tank contained a fungus and that the first primary filter was clogged by fungus. The other DG day tanks also contained a fungus and fungus spores were found in the main storage tanks. The fuel oil in the day tanks was diocided and filtered until the fuel oil met the criteria of STP M-108, "diesel fuel oil analysis," for particulate contamination, flash point, API gravity and viscosity. The day tanks were drained, inspected and cleaned. The bottom of main storage tanks 0-1 and 0-2 were suctioned out and a biocide was added. A biocide program will be developed and implemented to inhibit the growth of fungus in the DG fuel oil storage system. Also, a sampling and inspection program for the DG day tanks will be developed. Both will be incorporated into plant procedures.

h. It is not clear how the fire suppression (CO_2) system in the DG rooms responds to various levels of seismic event. The safety concern is that if an earthquake fails the diesel units without causing fire, one or more DG rooms might be flooded with CO_2, and therefore rescue personnel may not be able to recover the DGs within proper time intervals.

3.4 Audit Calculations

In order to scrutinize the quantified split fractions themselves, BNL performed audit calculations for each of the split fractions associated with each of the boundary conditions. The calculations were extended for both non-seismic (mission time: 6 hours) and seismic (mission time: 24 hours) cases. Seismic calculations were not performed for the Fuel Oil Transfer System. In these audit calculations the same assumptions, input data, maintenance and test frequency and duration, as well as mean fragility and human factor values were used as in the DCPRA. The SETS code[7] and locally generated PC software were used for the computations. The use of the SETS code allowed the identification of the most important cut sets contributing to the hardware unavailabilities. These cut sets are not readily accessible for direct review in the DCPRA. Appendix A lists the ranked cut sets for single, double, triple, quadruple and quintuple diesel failures. The definition of the basic events appearing in the cut sets are identical to those given in Chapter D.2.1.5 of the DCPRA.

The results obtained by the audit calculations are presented in Tables 2.6 and 2.7.b for the DGs and for the Fuel Oil Transfer System, respectively. They are denoted by "BNL" to be compared with the values given in the DCPRA (denoted by "PG&E"). It has to be emphasized, that if the review of the fragilities would identify incorrect values characterizing diesel components or the use of incorrect human failure rates would be detected during the review of the human factors, complete requantification of the Table 2.7.b split fractions would be necessary.

Table 3.1
Systems and Components Contributing Most to Failures
at All Types of DGs and at ALCO Type DGs

Systems and Components	Percent of All Failures		Percent of Failures at ALCO DGs	
Instrument and Controls System	25		26	
Governor		10		15
Sensors		3		3
Relays		2		1
Startup Components		2		1
Fuel System	11		10	
Piping on Engine		3		1
Injector Pumps		2		1
Fuel Oil Pumps				5
Starting System	10		6	
Controls		3		3
Starting Air Valve		2		
Starting Motors		2		2
Air Compressor		1		1
Switchgear System	10		10	
Breakers		3		4
Relays		5		4
Instrument and Controls		1		1
Cooling System	9		14	
Pumps		2		1
Heat Exchangers		2		1
Piping		2		6
Lubrication System	7		8	
Heat Exchangers		2		3
Pumps		2		3
Lube Oil		1		
Other Systems	28		26	

Date Base: 1984 failure event recorded between 1974 and 1984 in Reference 5.
Nuclear plants where ALCO Diesel Generators have been used in 1984:

Indian Point 1 and 2, Power Authority of the State of NY
Salem 1 and 2, Public Service Electric and Gas Company
Palisades, Consumers' Power Company
Pilgrim 1, Boston Edison
Ginna, Rochester Gas and Electric

REFERENCES

1. Final report on the Diablo Canyon Long-Term Seismic Program, Pacific Gas and Electric Co., Diablo Canyon Power Plant, Docket Nos. 50-275 and 50-323, July 1988.

2. Diesel Generator Allowed Outage Time Study, Pacific Gas & Electric Company, May 1989.

3. Units 1 and 2 Diablo Canyon Power Plant, "Final Safety Analysis Report Update," Pacific Gas and Electric Co., December 1988.

4. PG&E letters to NRC signed by J.D. Shiffer, No. DCL-88-238, October 10, 1988, No. DCL-88-260, October 28, 1988, No. DCL-88-285, November 29, 1988, No. DCL-88-297, December 9, 1988, No. DCL-89-010, January 16, 1989, and No. DCL-89-152, June 2, 1989.

5. Hoopingarner, K.R., Vause, J.W., Dingee, D.A., Nesbitt, J.F., "Aging of Nuclear Station Diesel Generators: Evaluation of Operating and Expert Experience," NUREG/CR-4590, August 1987.

6. DOE/RECON, Nuclear Safety Information Center (NSIC), 1963 to present.

7. Worrel, R.B. and Stack, D.W., "A SETS User's Manual for the Fault Tree Analyst," Sandia National Laboratories, NUREG/CR-0475, SAND77-2051, November 1978.

APPENDIX A

HARDWARE UNAVAILABILITY CUT SETS FOR THE DIESEL GENERATORS

Hardware Unavailability Cutsets in Case of One DG

Total Hardware, HW =

1	3.6736E-02	FIC1F +
2	2.1339E-04	HEV * FIV1F +
3	1.1073E-04	ODC +
4	1.1073E-04	ODA +
5	1.1073E-04	ODD +
6	1.1073E-04	ODB +
7	1.7703E-05	GDG +
8	1.6417E-05	TDA +
9	1.6417E-05	TDC +
10	1.6417E-05	TDE +
11	1.6417E-05	TDB +
12	1.6417E-05	TDF +
13	1.6417E-05	TDD +
14	5.8176E-05	HEV * DVC +
15	5.8176E-05	HEV * DVA +
16	5.8176E-05	HEV * DVD +
17	5.8176E-05	HEV * DVB +
18	4.1268E-07	HEV * TVA +
19	4.1268E-07	HEV * TVC +
20	4.1268E-07	HEV * TVE +

Independent Hardware, HWI =

1	3.6736E-02	FID1F +
2	2.1339E-04	HEV * FIV1F

July 25, 1989

Hardware Unavailability Cutsets in Case of Two DGs

Total Hardware, HW =

1	1.3495E-03	FID1F * FID1G +
2	1.1073E-04	DDA +
3	1.7703E-05	GDG +
4	1.6417E-05	TDB +
5	1.6417E-05	TDA +
6	1.6417E-05	TDC +
7	7.8392E-05	FID1F * HEV * FIV1G +
8	7.8392E-05	HEV * FIV1F * FID1G +
9	5.8175E-05	HEV * DVA +
10	4.0678E-06	FID1F * DDF +
11	4.0678E-05	FID1G * DDC +
12	4.0678E-06	FID1F * DDG +
13	4.0678E-05	FID1F * DDE +
14	4.0678E-05	FID1G * DDD +
15	4.0678E-05	FID1G * DDB +
16	1.1384E-05	HEV * FIV1F * FIV1G +
17	6.3309E-07	FID1F * TDI +

Independent Hardware, HWI =

1	1.3495E-03	FID1F * FID1G +
2	7.8392E-05	FID1F * HEV * FIV1G +
3	7.8392E-05	HEV * FIV1F * FID1G +
4	1.1384E-05	HEV * FIV1F * FIV1G

July 25, 1989

Hardware Unavailability Cutsets in Case of Five DGs

Total Hardware, HW =

1	1.7797E-05	GDG +
2	3.1996E-07	HEV * GFO +
3	6.6905E-09	FID1F * FID1G * FID1H * FID2G * FID2H +
4	2.2155E-08	FID1F * FID2G * TDH +
5	2.2155E-08	FID1G * FID2G * TDE +
6	2.2155E-08	FID1G * FID2H * TDD +
7	2.2155E-08	FID2G * FID2H * TDA +
8	2.2155E-08	FID1H * FID2H * TDB +
9	2.2155E-08	FID1F * FID2H * TDG +
10	2.2155E-08	FID1H * FID2G * TDC +
11	2.2155E-08	FID1G * FID1H * TDF +
12	2.2155E-08	FID1F * FID1H * TDI +
13	2.2155E-08	FID1F * FID1G * TDJ +
14	5.4896E-09	FID1G * FID2G * FID2H * DDB +
15	5.4896E-09	FID1G * FID1H * FID2H * DDC +

Independent Hardware, HWI =

1	6.6905E-09	FID1F * FID1G * FID1H * FID2G * FID2H +
2	3.8864E-10	FID1F * HEV * FIV1G * FID1H * FID2G * FID2H +
3	3.8864E-10	HEV * FIV1F * FID1G * FID1H * FID2G * FID2H +
4	3.8864E-10	FID1F * HEV * FID1G * FID1H * FID2G * FIV2H +
5	3.8864E-10	FID1F * HEV * FID1G * FID1H * FIV2G * FID2H +
6	3.8864E-10	FID1F * HEV * FID1G * FIV1H * FID2G * FID2H +
7	5.6439E-11	FID1F * HEV * FIV1G * FID1H * FID2G * FIV2H +
8	5.6439E-11	FID1F * HEV * FIV1G * FID1H * FIV2G * FID2H +

July 25, 1989

Enclosure 2

TOPICS FOR DISCUSSION

HUMAN FACTORS ANALYSIS

DIABLO CANYON PROBABILISTIC RISK ASSESSMENT (DCPRA)

1. It is stated in the DCPRA that SLIM-MAUD type algorithm was used to quantify human errors but neither the exact nature of the algorithm (how it differs from SLIM-MAUD and why) nor its conceptual foundation is described in the DCPRA report. However, our review of Appendix G does not clarify the derivation of SLIM-MAUD used in the analysis or its conceptual foundation. Additionally, it does not clarify how data from training simulators, and data collected directly from operator personnel (including their sampling) were used to index PSF values which supported human error quantification.

2. More discussions are needed to understand how the Human Cognitive Reliability (HCR) model was used to analyze recovery actions.

3. Discussions are needed as to whether human error was treated or not as a distal contributor (e.g., test and maintenance) to component failures and/or human errors probabilities input to the main accident sequences, and whether human error was treated or not as an immediate precursor (initiator) of the sequences themselves.

4. Discussions as to whether non-equipment centered PSFs (e.g., supervision, communications, coordination, other group processes) were considered or not in the HRA portion of the PRA.

5. The performance shaping factor survey forms (Section G.9 of the PRA) imply that if all the steps of an action are memorized that the action is skill-based. This does not seem in agreement with the basic tenets of the Human Cognitive Reliability (HCR) model. In this model, skill-based behavior is defined as well-practiced behavior. If an action is practiced at most once a year, then, even if the rules are memorized, it is not

skill-based behavior, but rather rule-based behavior.

If actions which are not routine actions, such as those performed in response to a fire, were never considered skill-based, but rather were considered rule-based (if procedures were available), what would be the approximate impact on the core damage frequency?

Enclosure 3

QUESTIONS ON THE FIRE ANALYSIS OF THE DIALBO CANYON PRA

1. On page F.3-16 it is stated that, given that CCW is lost to the RCP bearings, it is conservatively estimated that severe damage to the RCP pumps will occur if they are not stopped within 20 minutes. On the other hand, the Seabrook PRA indicates that (see p. 9.14-18 of the Seabrook PRA) loss of bearing cooling would lead to rapid and severe damage to the RCP seals, leading to a RCP seal LOCA, which would in turn lead to failure of the HPI pumps when they are started in response to the LOCA. In the Seabrook PRA, no credit was given for operator action to stop the RCPs before RCP seal damage occurs, for either control room fire sequences or cable spreading room fire sequences, because of the short time available.

   Justify the estimate that the RCP pumps can operate for twenty minutes without suffering severe damage, given a loss of bearing cooling.

2. On p. F.3-14 of the PRA, it is stated that a conservative assessment of the area fraction of the board VB-1 on which a fire could affect both the ASW and CCW control circuits is one third. Why could not a fire starting anywhere on the board VB-1 propagate to the locations of both the ASW and CCW circuits? Are there any barriers to the propagation of the fire from another portion of the board VB-1?

   Justify the factor of one third used for the area fraction.