A CONCEPTUAL DESIGN FOR

THE PALO VERDE NUCLEAR GENERATING

STATION

FOR A

DIVERSE AUXILIARY FEEDWATER

ACTUATION SYSTEM

(DAFAS)

PCR No. 89-13-SB-016
(DCP No. 1,2,3FJ-SB-064)

9008070071 900731
PDR ADOCK 05000528
P PDC

TABLE OF CONTENTS

DESIGN FOR A DIVERSE AFAS

I. INTRODUCTION

This conceptual design was prepared in support of plant change request 89-13-SB-016 to provide data associated with a detailed functional design for a Diverse Auxiliary Feedwater Actuation System (DAFAS). The design describes the current PVNGS Reactor Protection System (RPS) and Engineered Safety Features Actuation System (ESFAS) hardware configuration along with applicable design criteria. This information along with the 10CFR50.62 guidance (see Appendix A) and the identified potential designs addressed in the APS PCR No. 89-13-SB-016 is used as a basis to generate a detailed functional design for a DAFAS. The detailed design identified within depicts a system implementation configuration that addresses the requirements of 10CFR50.62, and which minimizes the impact of installation.

The DAFAS design addresses three major interfaces: 1.) the use of existing sensors, 2.) the DAFAS logic, and 3.) the interface with the Auxiliary Relay Cabinets (ARC). A key design basis of the DAFAS was that the DAFAS would be required only upon failure of the existing Plant Protection System for ATWS demands for Auxiliary Feedwater. This approach, therefore, eliminates the early assumptions on the part of the Combustion Engineering Owners Group (CEOG) that the DAFAS must be able to detect and isolate feed to a ruptured S/G in that a feedline/steam-line break scenario is not an Anticipated Operational Occurrence (AOO) concurrence. This position is also consistent with the NRC position as stated in References 1 and 4. The current Plant Protection System design protects against a ruptured S/G without the need for additional diversity. It is required, however, that the DAFAS not interfere with accident mitigation by the PPS therefore requiring an override or lockout of the DAFAS upon AFAS (Auxiliary Feedwater Actuation System) actuation.

II. EXISTING PVNGS PPS AFAS DESIGN

A. DESCRIPTION

The PPS maintains plant safety by monitoring various plant parameters, and initiating protective actions if any parameter exceeds its associated setpoint. The PPS consists of two separate but functionally similar systems: the RPS to trip the Reactor and the ESFAS to actuate the accident mitigation related equipment.

This effort is concerned with the Auxiliary Feedwater Actuation Signal (AFAS) generated in the ESFAS portion of the PPS.

The AFAS initiates auxiliary feedwater to the intact steam generator(s) following a low secondary inventory for whatever reason. It is initiated on a two out of four logic basis to a steam generator if that steam generator meets the conditions for either of the following:

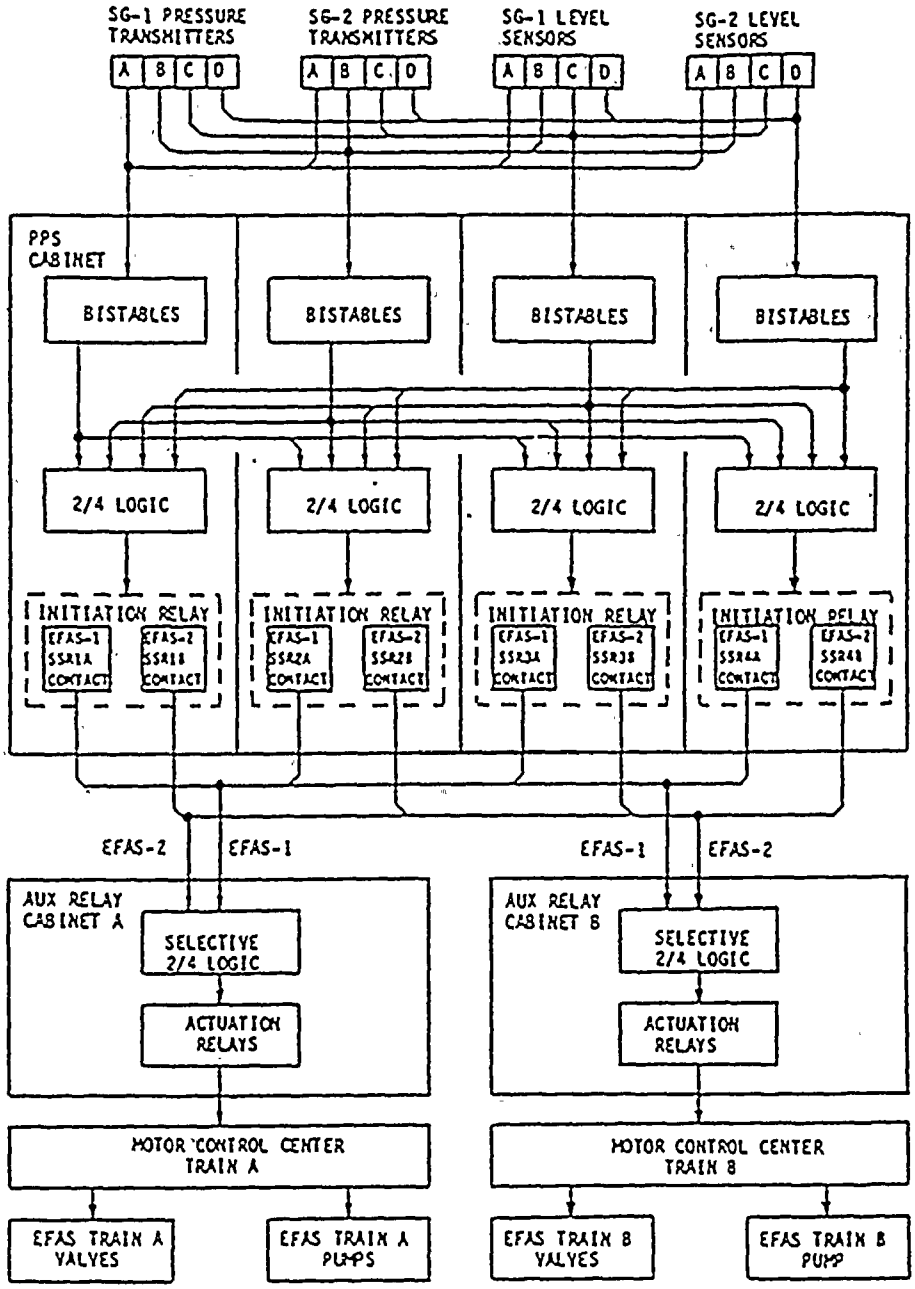
1) The steam generator's water low level trip exists without the low steam generator pressure trip present.

2) The steam generator's water low level trip exists and this steam generator's pressure is greater than the other by a predetermined differential pressure trip setpoint.

Separate actuation signals are provided for each steam generator. AFAS-1 pertains to steam generator No. 1 and AFAS-2 pertains to steam generator No. 2. The auxiliary feedwater discharge valves for each steam generator receive separate actuation signals from interposing relays in parallel with each AFAS-1 and AFAS-2 initiation circuit. This insures that the intact steam generator will receive auxiliary feedwater actuation signals and the non-intact steam generator will receive an isolation actuation signal upon receipt of a signal from the PPS.

The AFAS uses four input signals, Steam Generator Number 1 (SG-1) Pressure, Steam Generator Number 2 (SG-2) Pressure, SG-1 Water Level, SG-2 Water Level. Each input parameter is monitored on four isolated channels A, B, C, and D by the Bistable Trip Units. The SG-1 and SG-2 pressures are input to two additional bistables (see Figures II-1 & II-2) to determine which SG pressure is greater.

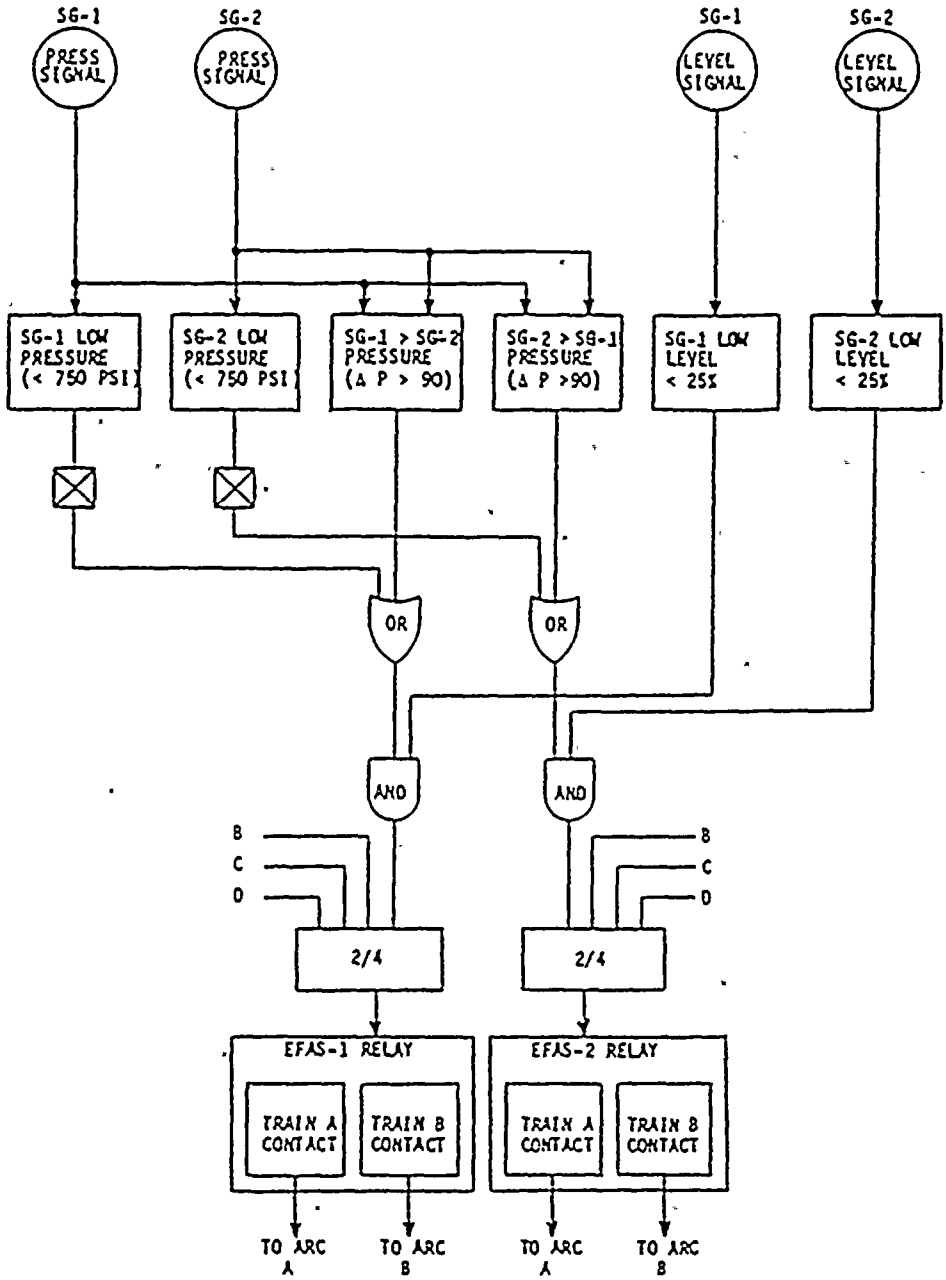
Each AFAS parameter input is represented as a voltage level. This voltage level is continuously compared to a pre-adjusted setpoint voltage, which itself represents the level at which trip response is necessary. If the parameter voltage becomes equal to the setpoint voltage, a trip bistable responds by generating a (bistable) trip output.



Title:

PPS SYSTEM BLOCK DIAGRAM

Figure II-1



Title:

PPS EFAS SIGNAL LOGIC DIAGRAM - CHANNEL

Figure II-2

A trip is considered valid when trip bistables are actuated simultaneously on two channels. The bistable trip outputs are applied to the PPS "two-out-of-four" coincidence logic matrices. These matrices are designed to account for all possible 2/4 combinations of the monitoring channels; they are designated AB, BC, BD, AC, CD and AD. A matrix generates a trip only if bistable trip receipt occurs on both matrix channels. The trip is then recognized as valid, and is applied to four PPS trip paths.

Each trip path includes six sets of relay contacts - each set controlled by a unique matrix. A trip path is activated by transferring (opening) any single contact set. Transferring these contacts enables trip response by a Trip Path Relay.

The trip path controls the solid state Initiation Relay which contains two contacts SSR(X)A and SSR(X)B. Where (X) is 1, 2, 3, or 4 corresponding to channels A, B, C, and D, respectively. The SSR(X)A and SSR(X)B contacts are sent to the Auxiliary Relay Cabinets (ARC) A and B where the Actuation Relays are located. These relays are normally energized and deenergize upon a trip. The contact outputs from these relays are sent to the Motor Control Center which controls the valves and pumps for the Steam Generator Feedwater. ARC A initiates actions for SG-1 and ARC B initiates actions for SG-2.

III. DIVERSE AFAS SYSTEM

A. FUNCTIONAL DESCRIPTION

The Diverse Auxiliary Feedwater Actuation System (DAFAS) consists of sensors, signal conditioning, trip recognition, coincidence logic, initiation logic, and other circuitry and equipment needed to monitor plant conditions and effect auxiliary feedwater actuation during conditions indicative of an ATWS. The intent of the Diverse Auxiliary Feedwater Actuation is to mitigate ATWS event consequences. This actuation action is provided during an Anticipated Operational Occurrence (AOO) requiring auxiliary feedwater coincident with a failure of the Plant Protection System (PPS) and indication of initiation of the Diverse Scram System (DSS).

The purpose of a Diverse Auxiliary Feedwater Actuation is to provide equipment to comply with the requirements of the ATWS Rule, 10CFR50.62. The actuation of the Auxiliary Feedwater System through the DAFAS provides a diverse means of event mitigation for those ATWS events.

The DAFAS initiation signals cause actuation of the auxiliary feedwater pumps and valves only if there is a demand for auxiliary feed and an AFAS signal has not been generated by the PPS. The occurrence of the AFAS signal by the PPS concurrent with the absence of an enable from the DSS indicates that conditions indicative of an ATWS have not occurred and Auxiliary Feedwater Actuation by the DAFAS is not necessary. Under these conditions the DAFAS actuation will be blocked through logic in the Auxiliary Relay Cabinet.

The functional requirements for the DAFAS include:

- DAFAS must initiate auxiliary feedwater flow for conditions indicative of an ATWS where the AFAS has failed.

- The DAFAS will not be required to provide accident mitigation such as isolation feed to a ruptured steam generator.

- DAFAS will secure feeding the affected steam generator(s) when reaching a pre-determined level setpoint (approximately 30 minutes after actuation) after which manual operator intervention will control the system.

- DAFAS will utilize logic and redundancy to achieve a 2-out-of-2 initiation, as a minimum.

- DAFAS will utilize steam generator level as the parameter indicative of the need for AFAS actuation.

- DAFAS will interface to the actuated components via the existing Auxiliary Relay Cabinet (ARC) relays.

- DAFAS will be blocked by the AFAS to prevent undesired interactions during non ATWS event, and to disable DAFAS when the AFAS system actuates.

- DAFAS will be blocked by the MSIS signal to prevent undesired interactions during non ATWS events and to disable the DAFAS when conditions for MSIS exist.

- DAFAS will be enabled by an enable signal, indicating DSS actuation, from the Supplementary Protection Logic Assembly (SPLA).

- DAFAS will include testing capabilities that allow testing to occur at power.

- DAFAS includes features that provide annunciator, plant computer and operator interface to allow for system status and operability requirements.

- DAFAS setpoints will be lower than the PPS setpoints so that a race condition between the PPS and DAFAS may be prevented.

- DAFAS will be built and qualified to meet the applicable design requirements for safety related equipment.

B. SYSTEM DESCRIPTION/FEATURES

The DAFAS cabinets contain the logic that determines if conditions exist for a DAFAS initiation. The DAFAS interfaces with the Process Equipment Cabinet(s) and the Auxiliary Relay Cabinet(s). The block diagram shown in Figure 1 depicts the overall configuration of one channel, Channel A, for the DAFAS system and the interfaces with the Process and Auxiliary Relay Cabinets (ARC).

Each DAFAS channel receives 8 inputs for a total of sixteen 16 inputs from the Process Cabinets, eight (8) level sensor inputs from each Steam Generator. The level inputs used are the existing narrow range level signals used by the PPS and located in the Process Cabinets. Each input signal is interfaced and isolated by use of a Fiber Optic (F.O.) Transmitter module where it is converted from an analog voltage signal to an optical signal. Each of the sixteen (16) level signals is transmitted to the DAFAS cabinets on a separate F.O. Cables.

The Steam Generator Level input signals are received by F.O. Receiver modules at the DAFAS cabinet where they are converted to an analog voltage signal and provided to each of the DAFAS Programmable Logic Controllers (PLC). Each channel of the DAFAS contains two PLC's which provide the capability of on-line testing without causing train actuation. Each PLC in the channel will process the same input signals and compare them to predetermined setpoints to determine if a DAFAS trip condition exists. If a trip condition exists, each PLC transmits a signal across two (2) F.O. serial data links, one for ARC A and one for ARC B, to I/O Systems located in the ARC. The I/O System receives the signal from the DAFAS and generates a contact output to initiate auxiliary feedwater flow.

Since the DAFAS System for PVNGS is to be safety related, then one (1) channel of the DAFAS must be able to initiate auxiliary feedwater flow. To achieve this requirement, the two PLC's in each channel are configured such that PLC 1 (A1 and B1) controls the 1-3 trip leg for AFAS 1&2 in ARC A&B and PLC 2 (A2 and B2) controls the 2-4 trip leg for AFAS 1&2 in ARC A&B.

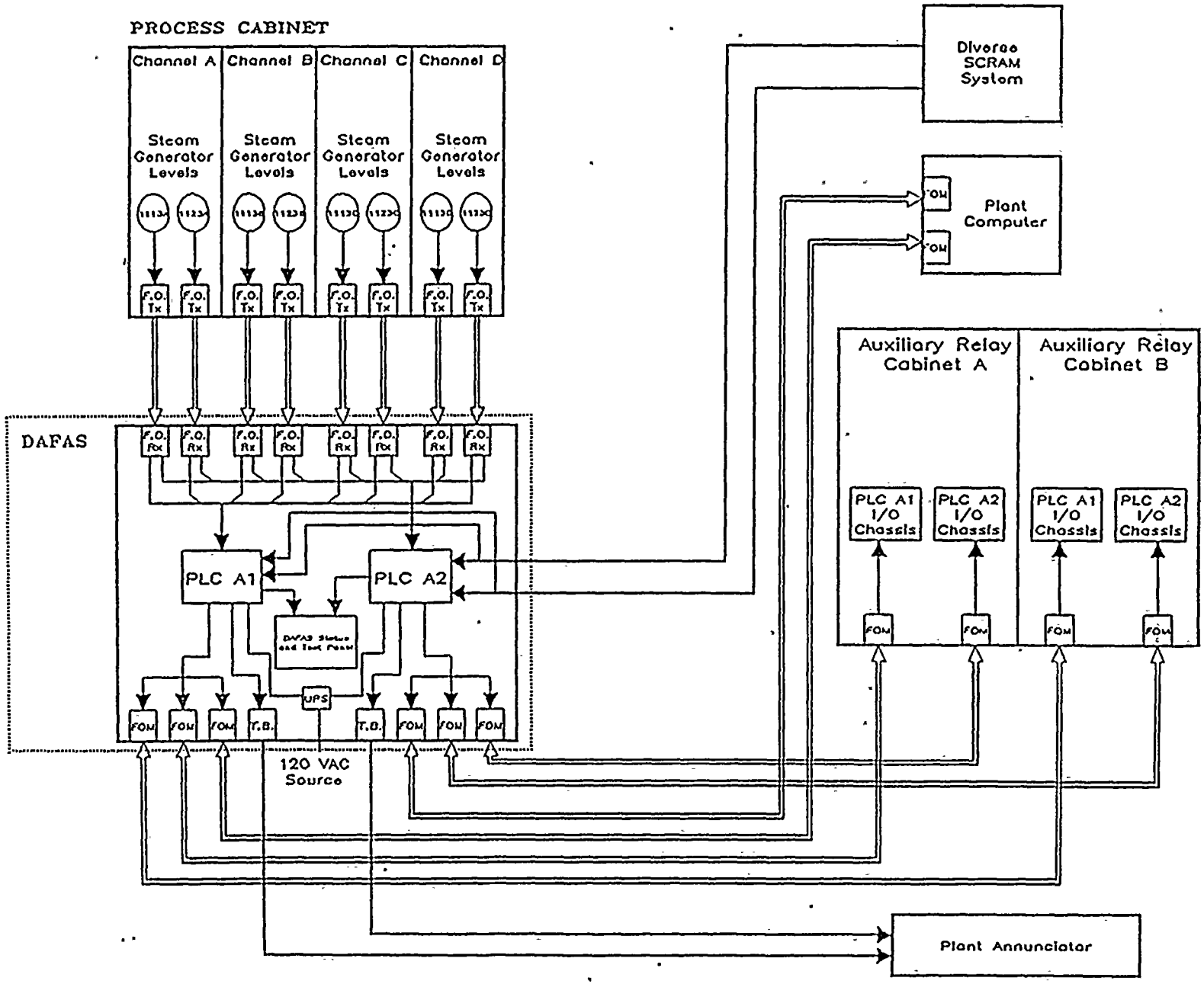
The DAFAS cabinet will also contain testing capabilities and local indication so that the state of the DAFAS can be easily determined. The testing capabilities at the DAFAS cabinet and Auxiliary Relay Cabinets are discussed in detail in Section III.F.

C. SYSTEM INTERFACES

This section describes in more detail each of the interfaces with the DAFAS; the sensors, the DAFAS cabinet, the Auxiliary Relay Cabinet.

Figure 1

DAFAS CHANNEL A SYSTEM DIAGRAM



1. SENSORS

The DAFAS uses four (4) narrow range safety channel level sensor inputs from each of the Steam Generators. These level signals are input to an analog Fiber Optic Transmitter module which converts the analog voltage signal to an optical signal for transmission to the DAFAS over F.O. cables. These F.O. Transmitter modules provide the isolation between the channelized Class 1E input signals and the 1E DAFAS.

There are a total of sixteen (16) F.O. Transmitter modules to be mounted in the Process Cabinet(s), four (4) in each of Channels A,B,C,& D. The F.O. Transmitter modules are compact in size (approximately 4"x4"x1") requiring little space for mounting in the Process Cabinets. These F.O. Transmitter modules are to be powered from the existing 24 Vdc power located in each channel of the Process Cabinets. The F.O. Transmitter modules are seismically and environmentally qualified to the same qualification standards as the PPS. The F.O. transmitter modules are qualified so that they will not degrade the current qualification standards of the Process Cabinets.

DAFAS LOGIC

The DAFAS logic will be designed and constructed consistent with the requirements of a safety related system and will consist of F.O. Receiver modules, F.O. modems, Power supplies, Uninterruptable Power supplies, Test/Indicator panels, I/O modules, and PLC's as shown in Figure 2. The DAFAS logic will be supplied in two wall mount enclosures (each approximately 30"W x 60"H x 16"D) for all of the equipment.

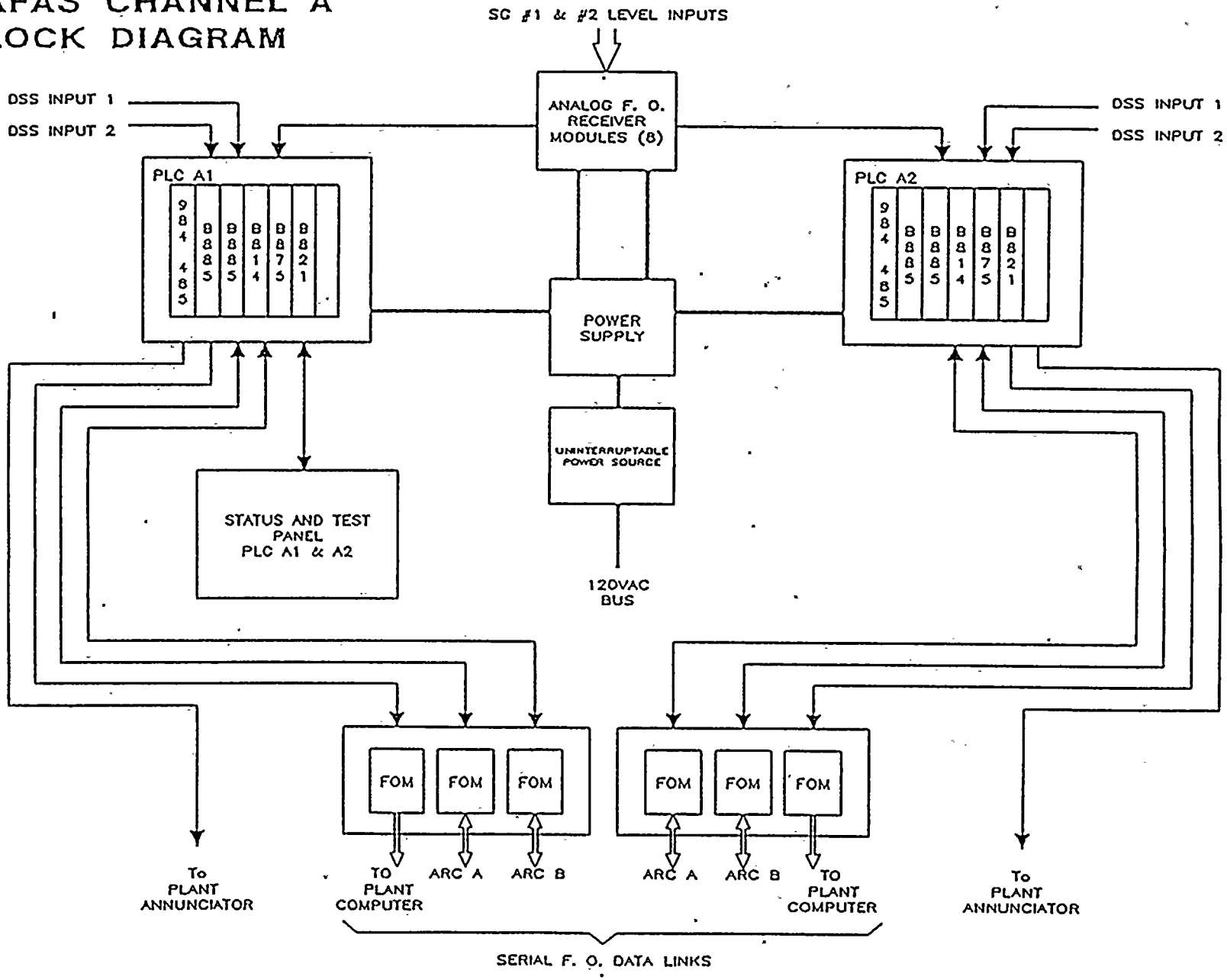
The DAFAS logic equipment will be qualified to the requirements of safety related 1E equipment including; seismic, environmental, EMI, fault testing, and will have undergone an extensive V&V program.

Each of the DAFAS logic systems contains eight (8) F.O. Receiver modules that convert the optical input signals from the Process Cabinet F.O. transmitter modules to analog voltage signals. The eight (8) analog signals are input to the two (2) PLC systems which perform the logic to determine if conditions for a DAFAS initiation exist. The F.O. Receiver modules contain a fault indicator LED and contact output that is activated upon loss of the optical signal (i.e. severed F.O. Cable). This fault indication is provided to assist in troubleshooting any problems that may be encountered with the input signals.

Each channel of the DAFAS contains an Uninterruptable Power Supply (UPS). The two UPS's receive power from separate 120 VAC vital buses. The UPS's are sized to supply power to the DAFAS logic for up to 1 hour following the loss of the 120 VAC vital buses.

In a DAFAS channel, each UPS supplies 120 VAC to a PLC chassis. Each UPS also supplies 120 VAC to a DC power supply. DC output voltage from each of the two (2) power supplies is auctioneered and supplied to the eight analog

FIGURE 2
DAFAS CHANNEL A
BLOCK DIAGRAM



F.O receiver modules and four (4) RS-232 F.O. modems which communicate with the DAFAS interface devices in the ARCs.

There are two channels used in the DAFAS for the purpose of redundancy and testing capabilities at power. PLC's A1 and B1 provide DAFAS 1 & 2 output signals for the 1-3 AFAS 1 & 2 Trip Legs and PLC's A2 and B2 provide DAFAS 1 & 2 output signals for the 2-4 AFAS 1 & 2 Trip Legs in the Auxiliary Relay Cabinet as shown in Figure 3. Putting one of the channels into test will not result in initiating feedwater flow as a DAFAS signal from both PLC's is required to cause a feedwater flow. A DAFAS signal from one of the PLC's results in one ARC trip leg, 1-3 or 2-4, to be tripped. However both trip legs are required to be tripped in order to drop out the subgroup relays resulting in feedwater flow.

The DAFAS configuration is based on the AEG Modicon 984 series Programmable Logic Controller (PLC) as shown in Figure 4.

The isolated analog input signals (0-10 Vdc) are directed to analog input modules (P/N B875) where A/D conversion is performed. Digitized analog values are automatically reported to the PLC upon interrogation during each PLC scan cycle. Analog input modules include self-test and auto calibration features to eliminate the need for periodic calibration of inputs. Each module contains a precision reference voltage source against which automatic calibration of each input signal is performed. This reference voltage source requires calibration on an annual basis. The converted analog values are compared to adjustable setpoints in the PLC processor (P/N 984-485) and bistable trip signals are generated when the setpoints are exceeded.

DSS trip status signals (24 Vdc) are received by digital input modules (P/N B821) and logically combined with bistable trip status signals (2/4 logic) in the PLC processor to generate DAFAS trip demand signals.

DAFAS trip demand is directed to ARC interfaces via RS-232 fiber optic isolated datalinks. These datalinks are supported by ASCII RS-232 modules (P/N B885) in the PLC chassis. In the ARCs, trip demand is received by high speed logic modules (P/N B984) which interrupt power to the existing 1-3 or 2-4 trip paths through interposing relays. These high speed logic modules also accept AFAS and MSIS actuation status signals from the ARC and direct them back to the PLC processor to block DAFAS actuation as required.

The DAFAS logic cabinets also include additional ASCII RS-232 modules and fiber optic modems to facilitate isolated datalink communication with the Plant Computer. Contact outputs are provided to the Plant Annunciator system via relay output modules (P/N B814) in the PLC chassis.

There is one (1) Status and Test Panel located in each DAFAS Cabinet. As shown in Figure 5, each panel contains a digital panel meter, 9 position keypad, 4 additional switches, and indicators. The keypad allows the operator to query a PLC to display the inputs and setpoints in the PLC on

the digital panel meter. The panel contains DAFAS 1 TEST and DAFAS 2 TEST test switches which are used to test the actuation logic in each PLC. The indicators on the test panel display the status of the DAFAS.

3. AUXILIARY RELAY CABINET

Each Auxiliary Relay cabinet contains four (4) I/O systems, two interfacing with A (PLC A1 and PLC A2) two with B (PLC B1 and PLC B2). These I/O systems are to be qualified to meet or exceed the qualification requirements of the Auxiliary Relay Cabinet so that they will not degrade the existing qualification of the Auxiliary Relay Cabinet.

The I/O systems consist of Fiber Optic Modems, high speed logic modules (P/H B984) with Digital Input and Output Capacity, Interposing Relays, and power supplies. The I/O systems are located in Bay 5 and Bay 8 of each Auxiliary Relay Cabinet. Bay 5 will also contain an indicator panel, see Figure 6, mounted below the ARC Test panel so that it can be easily observed during testing.

The I/O system interfaces with the current logic of the Auxiliary Relay Cabinet as shown in Figure 3. The I/O system receives inputs from DAFAS through a serial F.O. data link. The I/O system then generates digital outputs that control the DAFAS 1 & 2 relays. Two other relays are installed in the Auxiliary Relay Cabinet to provide a bypass function that will disable the DAFAS system when desired.

The I/O system receives inputs that are available to be read by the PLC through the serial data link. These inputs include AFAS and MSIS lockout relay status, test input, and a bypass input.

The Bay 5 I/O system interfaces with the indicator panel directly however the bay 8 I/O system sends digital inputs back to Train B (PLC #2) which transmits these Digital inputs to Train A (PLC #1). PLC #1 then sends the Digital Outputs to the I/O system in Bay 5 which controls the Indicators for the PLC #2 I/O system.

D. SYSTEM SOFTWARE

DAFAS software will be developed and verified in accordance with the methods defined by References 2 and 3. These computer software control procedures apply to Class 1E Safety-Related Systems, to assure that the system will perform its function in a reliable manner.

DAFAS software execution is deterministic (i.e., repetitive and non-interrupt driven) to ensure predictable system performance and response under worst-case loading conditions.

Software is classified into two major categories; operating system software and application software. Operating system software consists of the PLC processor operating system, I/O handling, communications handling and equipment self-test software. Application software is the implementation-specific code that is developed during the DAFAS design process.

Operating system software code resides in fixed read only memory (ROM) within the PLC processors. This code is written by the PLC manufacturer and offered as a standard off-the-shelf product. Qualification is accomplished by a combination of a) validation through extensive testing for the intended application and b) successful operating history in similar applications. After qualification testing, stringent configuration controls are maintained for the operating system software.

Application software code resides in battery-backed non-volatile random access memory (RAM) in the PLC processors. This code is written during the DAFAS design process in PLC relay ladder logic (RLL) language. The application software development task is divided into manageable subtasks referred to as software modules. Upon completion, each software module is subjected to independent review to determine that functional requirements are met. Software module operation is then validated by extensive and thorough testing. Software modules are then integrated and the independent review process and test process is repeated for integrated system operation. Software certification is awarded upon completion of this process.

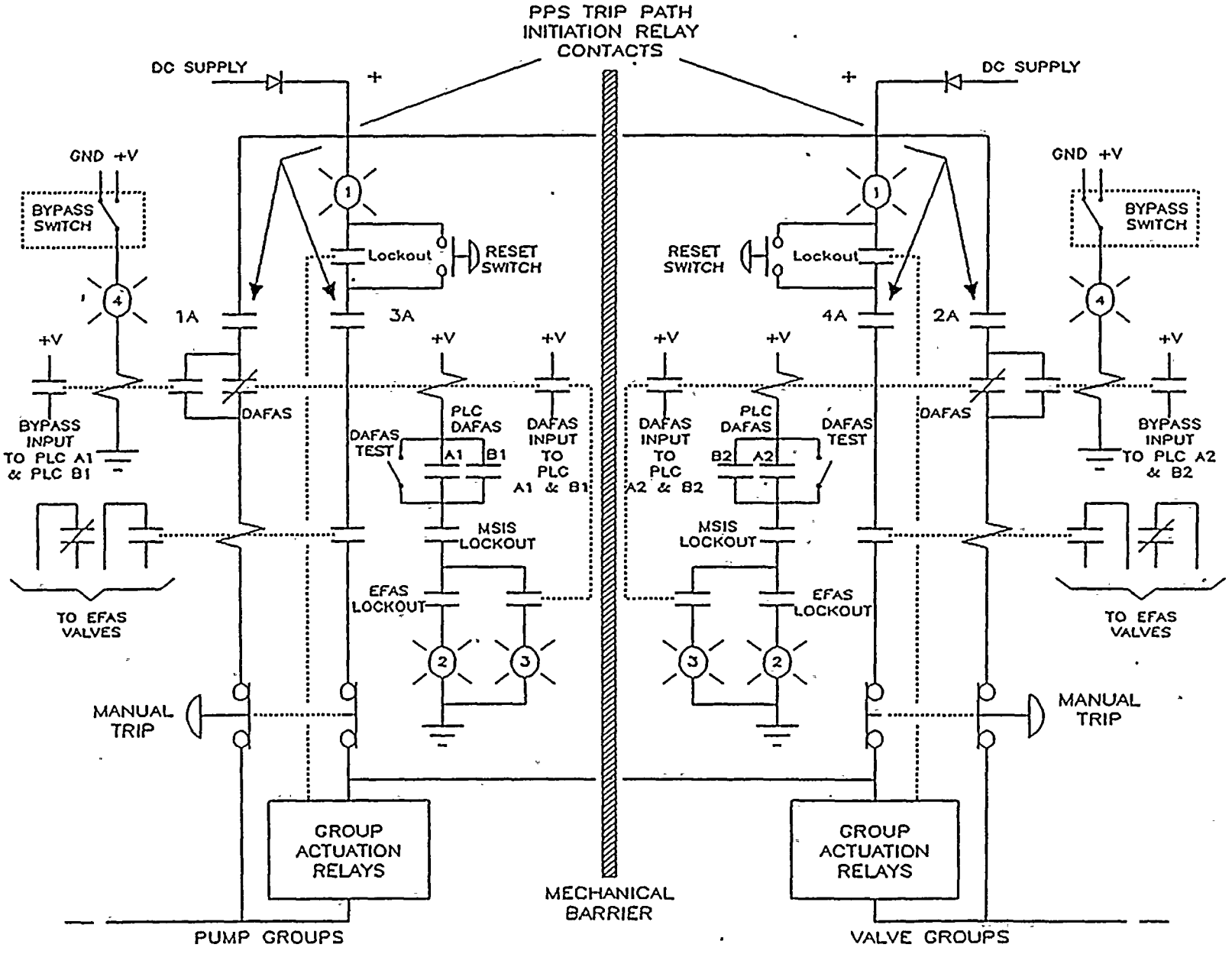
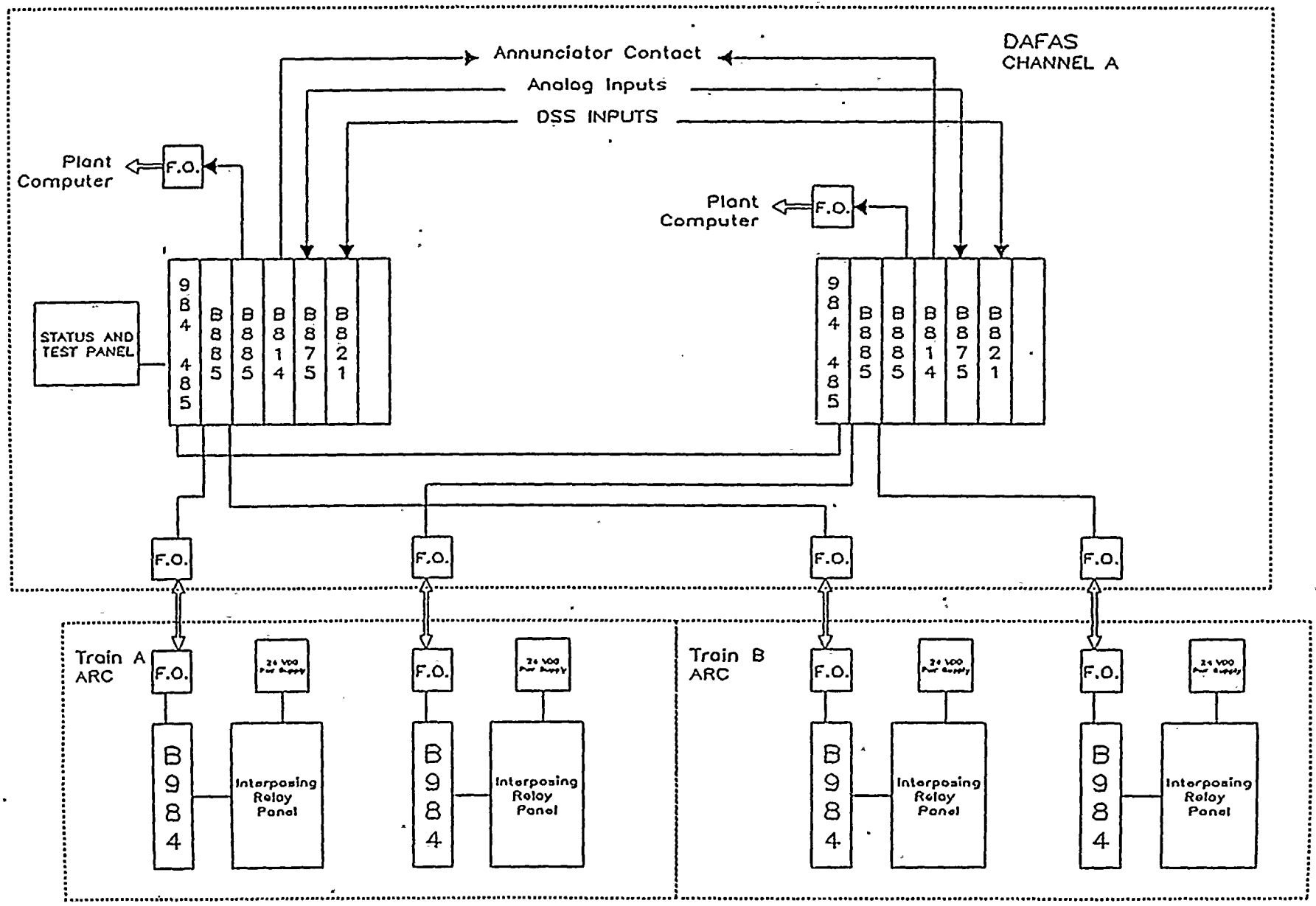


FIGURE 3
ESFAS AUXILIARY. RELAY CABINET
SIMPLIFIED FUNCTIONAL DIAGRAM

FIGURE 4
DAFAS HARDWARE CONFIGURATION



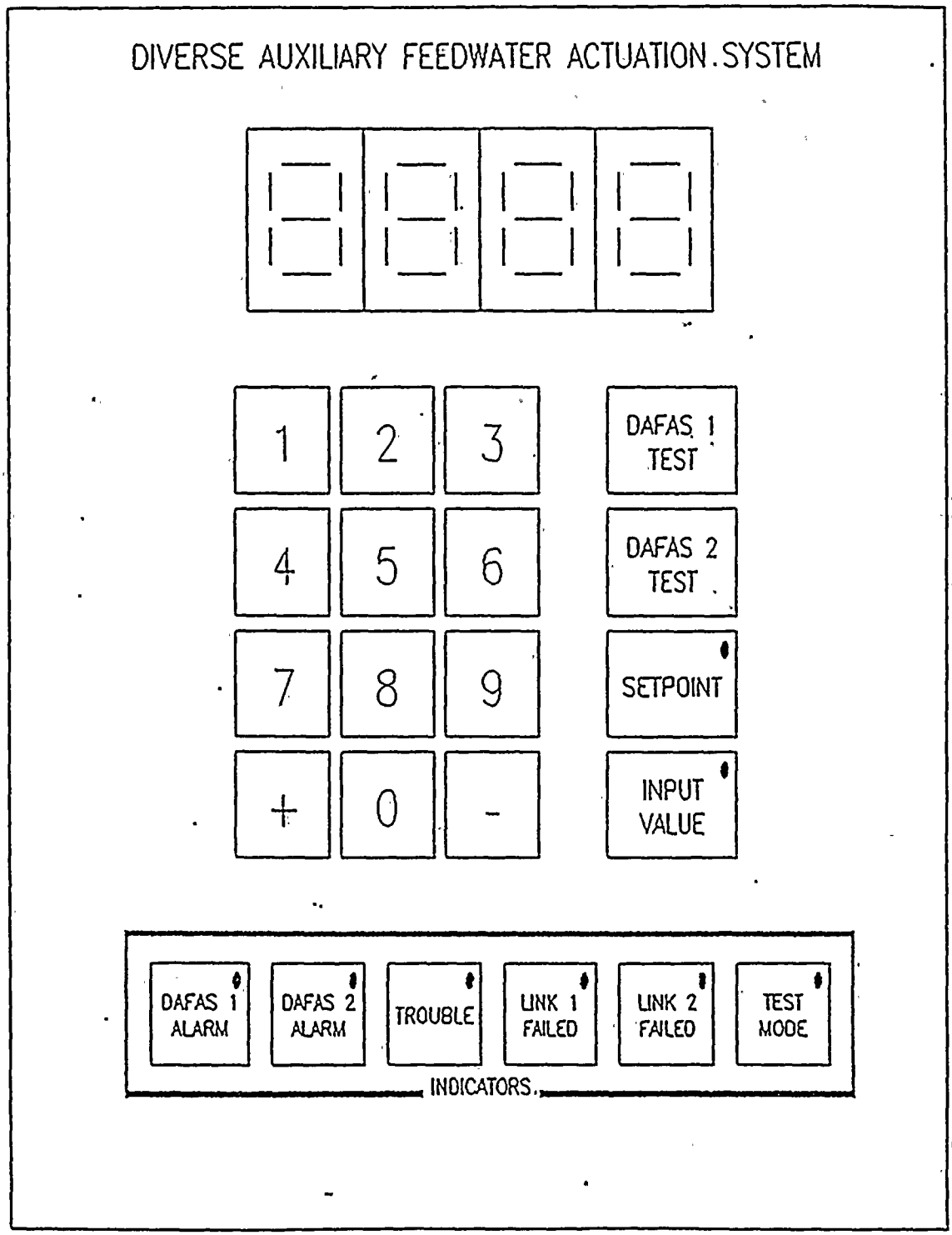


FIGURE 5
DAFAS STATUS AND TEST PANEL

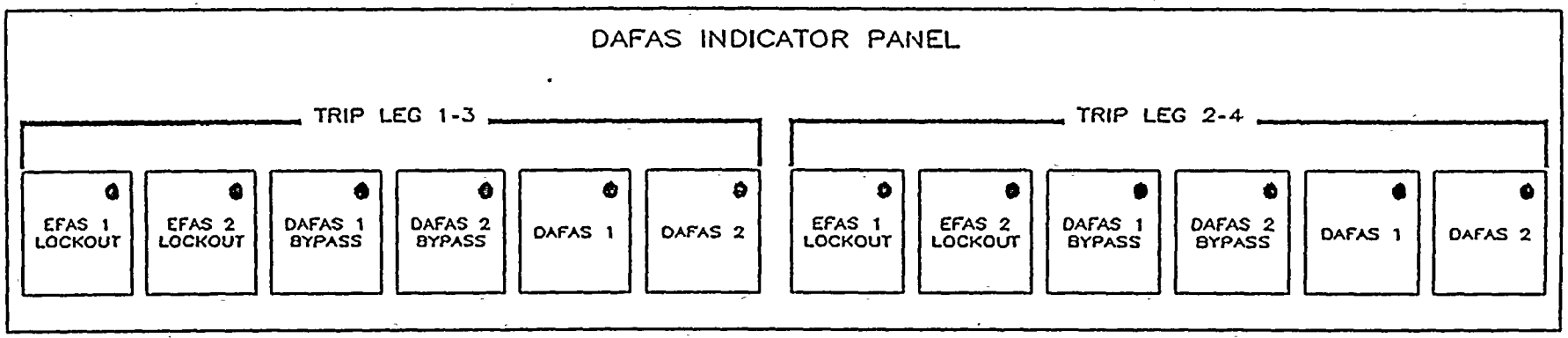


FIGURE 6
TYPICAL DAFAS INDICATOR FOR AUX RELAY CABINET

E. DETAILS OF OPERATION

DAFAS provides two (2) redundant channels of equipment, either train having the capability of completely actuating auxiliary feedwater to both steam generators on demand. For clarity one channel is described below.

Each of the DAFAS Logic Systems receives eight (8) level sensor inputs from each Steam Generator. These signals are compared to a setpoint to determine if the level in the Steam Generator is too low. This setpoint is set to a value below the setpoint used in the PPS. The intent of the lower setpoint is to prevent a race condition so that the DAFAS will not initiate feedwater flow before the ESFAS when the ESFAS is operating normally.

Each of the DAFAS PLC's use a 2-out-of-4 (2/4) sensor logic calculation on the Steam Generator Level Signals. If any two (2) of the four (4) Steam Generator #1 Level Signals indicate low level and a DSS actuation has occurred then the DAFAS will generate a DAFAS signal to the ARC. The same logic is used for the Steam Generator #2 level inputs.

The DAFAS PLC outputs are actually set up as a 2/2 logic system where a DAFAS signal from both PLC's is required to initiate feedwater flow. A DAFAS signal generated by one PLC will only result in controlling the cycling relays that control feedwater valves to the Steam Generators. The DAFAS logic in the ARC (see Figure 3) is designed such that the loss of both trip legs, 1-3 and 2-4, are needed to deenergize the subgroup relays, resulting in feedwater flow to the Steam Generators.

The DAFAS receives digital inputs from the Diverse Scram System (DSS) which indicate that the DSS has actuated. These inputs allow the DAFAS to initiate feedwater flow only if a DSS actuation has occurred. These inputs are provided to prevent a DAFAS inadvertent actuation from occurring.

The DAFAS contains an error checking routine to detect the loss of a serial link to the I/O System in the ARC. If the PLC determines the link has failed it will turn on an indicator at the status and test panel to indicate a failed link (i.e. Link 1 failed, Link 2 failed).

The F.O. Receiver Modules in the DAFAS contain fault logic to detect the loss of an input signal. A fault LED on the Receiver Module is lit and a relay output is generated by the F.O. Receiver Module to indicate the fault condition.

Automatic Testing - All of the Modicon processors in the system include automatic testing of the hardware and software to identify problems within the equipment that might prevent it from performing its intended function. The tests include power-up and on-line testing.

Power-Up Testing - Upon power-up, complete diagnostics are performed on all hardware including processor and memory. The types of diagnostics include:

A. Test of the CPU.
B. Checksum test of the controller's system programs.
C. Checksum test of user logic memory.
D. Checksum test of I/O and register storage allocation.
E. Test of volatile memory using read/write tests.
F. Check of stored configuration against what is found to be installed.
G. Communication checks to I/O units and other attached processors.

On-Line Testing - To verify each controller's ability to perform its function, background diagnostics are performed during each cycle of the controller sequence. Background diagnostics are executed during each sequence. The background diagnostics are similar to power-up diagnostics but are not as extensive. They are sufficient to determine that the software is unaltered and that the hardware is operating properly. Some of these tests and checks are discussed below:

A. Memory Test

Memory which is used for inputs, outputs, internal logic states and/or values is write-read checked to verify that it has not failed in an unalterable state.

B. Program Logic Testing

The program logic is continually monitored to ensure it is unchanged from the logic that was originally loaded into the processor. This is accomplished by calculating the checksum for the logic in the processor. The calculated checksum is then compared with the checksum for the logic that was originally loaded. Any discrepancy between the checksum of the logic and the precalculated value will result in an error condition. The checksum is of the CRC variety thus precluding multiple errors from masking each other and going undetected.

C. Communication Checks

All communications include a means of ensuring that the received data is accurate. The methods used to ensure this accuracy include, block or packet headers which identify source and destination, checksums and parity checks. In some cases multiple transmissions are made and two identical transmissions must be received before the data is actively used. When errors in transmission occur, the data is not updated. After several transmission errors occur, an alarm is generated.

When a trip signal is received by the I/O system, the I/O system generates a digital output that drives the DAFAS Relay which causes a trip to occur. Figure 3 shows the logic of the DAFAS circuit in the ARC.

The I/O systems for PLC's 1&2 interface with an Indicator Panel. The Indicator Panel is to be mounted near the Test panel so that it can easily be seen during testing. The Indicator Panel indicates the states of the various relays involved in the DAFAS Actuation circuit.

Each I/O system in the ARC generates two trip signals, DAFAS 1 and DAFAS 2. Two bypass switches are located near each I/O system to bypass the DAFAS 1 and DAFAS 2 Trip Signals. When this switch is activated, an indicator on the Indicator Panel lights to annunciate the bypassing of the DAFAS outputs.

The logic for the DAFAS Relays is shown in Figure 3. The DAFAS Relay will be energized only if the MSIS Lockout and AFAS Lockout Relays are closed (normal position). If either the MSIS Lockout or AFAS Lockout Relays are open, the DAFAS cannot initiate feedwater. The Lockout Relays being open indicates that the PPS is operating normally and has already initiated feedwater flow or isolated a ruptured S/G and thus blocks the DAFAS since conditions for DAFAS do not exist.

The MSIS signal initiates isolation of each Steam Generator to rapidly terminate blowdown and feedwater flow if a steamline rupture occurs. The PPS MSIS logic uses the Steam Generator pressure inputs to determine if conditions for MSIS are present. The MSIS lockout relay is used as a blocking signal for the DAFAS so that if a steamline rupture occurs, the DAFAS will be unable to initiate feedwater flow. Feedwater flow to a ruptured steamline is not a desirable event.

If the MSIS and AFAS Lockout Relays are closed, then the DAFAS can initiate a one cycle feedwater signal. This means that when the DAFAS initiates Auxiliary Feedwater the DAFAS Relay is energized and one of the contacts is wired to bypass the AFAS Lockout Relay contact. This bypass is necessary because when a DAFAS is initiated the AFAS Lockout relay will open and latch which, if it is not bypassed, would prevent the DAFAS from controlling feedwater flow. After the steam generator level is restored to a predetermined setpoint, the DAFAS will open its contact deenergizing the relay and securing auxiliary feedwater flow to the steam generator. This disables the bypass on the AFAS Lockout Relay and since this is a Latching Relay it will remain open until it is manually reset by the operator. This will prevent the DAFAS from initiating a second auxiliary feedwater flow. One cycle will take approximately 30 minutes or more for the steam generator level to return to normal level. This will allow the operator sufficient time to take control of the feedwater system and perform the necessary actions to continue operation of the system.

F. TEST CAPABILITIES

The DAFAS has test capabilities at both the DAFAS Cabinet and at the ARC.

The Status and Test Panel for the DAFAS Cabinet is shown in Figure 5.

The keypad allows the operator to select any analog input and displays its input value or setpoint on the digital display. Two switches next to the keypad contain lamps to indicate which value is being displayed. If the setpoint switch is depressed, the setpoint value is displayed, if the input value switch is depressed, the input value is displayed. These values can be displayed at any time it is desired whether in test mode or in normal operation.

Two other switches on the test panel, DAFAS 1 TEST and DAFAS 2 TEST, are used to test the actuation logic. When the DAFAS 1 TEST or DAFAS 2 TEST switch is depressed, the PLC sends a DAFAS actuation signal to the ARC causing the DAFAS Relay to energize. A digital input to the I/O system is generated by the DAFAS Relay indicating that the relay has actuated. The PLC reads the input from the I/O system and turns on the DAFAS 1 or 2 indicator on the test panel. This indicates that the actuation logic and DAFAS relay is working correctly.

There are also test capabilities provided at the ARC for checking relay operation during the ARC periodic testing. The DAFAS Indicator Panel is located below the ARC test panel for easy viewing when testing.

The testing for the relays in the ARC involves looking at the indicator lights to determine the state of the relays. Typical test and indication sequence would be as follows:

AFAS Phase Action	Resulting Light Status		
	DAFAS 1	Lockout	Current
Normal Conditions	OFF	OFF	ON
Depress DAFAS 1 Test Switch	ON	ON	OFF
Initiate MSIS	OFF	OFF	ON
Release MSIS	ON	ON	OFF
Release DAFAS 1 Test Switch	OFF	OFF	ON
Depress DAFAS 1 Test Switch	ON	ON	OFF
Initiate AFAS	ON	OFF	OFF
Release AFAS	ON	ON	ON
Release DAFAS I Test Switch	OFF	OFF	ON
Initiate AFAS	OFF	OFF	ON
Depress DAFAS I Test Switch	OFF	OFF	ON
Release DAFAS I Test Switch	OFF	OFF	ON
Release AFAS	OFF	OFF	ON

This testing was designed such that it could be incorporated into existing ARC Test Procedures in such a manner as to keep the cycling of the relays

and components to a minimum.

IV. 10CFR50.62 COMPLIANCE

The DAFAS is designed to be in accordance with the guidelines set forth in 10CFR50.62. These guidelines are described in Appendix A. The DAFAS meets the guidelines as described below:

Safety Classification

The DAFAS consists of three (3) groupings of equipment, the F.O. Transmitter Modules, the DAFAS Cabinet, and the I/O system in the ARC.

The DAFAS Cabinet is designed as a safety related control system. This exceeds requirements of 10CFR50.62 and provides enhanced operability and availability.

The Transmitter Modules in the Process Cabinets and the I/O system in the ARC are considered safety related equipment in that they must not degrade the design requirements of the interfacing system(s) and they are located in safety related cabinets.

Redundancy

The DAFAS is not required to contain redundancy.

Separation from Existing System

The DAFAS is fiber optically isolated via qualified devices and physically and electrically separate from the existing PPS. It does not degrade the existing separation criteria of the PPS or ARC.

Environmental Qualification

The DAFAS Cabinet will be environmentally qualified for those conditions that may be expected to occur during an AOO. It is environmentally qualified for other accident conditions consistent with the requirements of the interfacing equipment. The F.O. Transmitter Modules in the Process Cabinet and the I/O System in the ARC are to be environmentally qualified for both the environmental conditions resulting from the AOO's and accident conditions. The environmental qualification will meet or exceed those of the existing ARC and Process Cabinets so as not to degrade the qualifications of those systems.

Seismic Qualification

The DAFAS Cabinet is not required to be seismically qualified to operate during a seismic event, but will be seismically qualified to enhance system performance and reliability and to ensure that it will not degrade other safety systems, installed in the same area, during a seismic event.

The F.O. Transmitter Modules in the Process Cabinet and the I/O system in the ARC will be seismically qualified to meet or exceed the qualification criteria of the existing Process Cabinets and ARCs so as not to degrade the qualification of those systems and to maintain isolation capability during a seismic event.

Quality Assurance

The DAFAS will be designed under the suitable Quality Assurance Procedures consistent with the requirements of 10CFR50, Appendix B.

Safety Related Power Supply

The DAFAS logic power supplies located in the DAFAS Cabinet, while not required, will be safety related. Each DAFAS logic power supply is interfaced with its own Uninterruptable Power Supply that is capable of providing 120 VAC power for up to one (1) hour following the loss of the 120 VAC power bus. This design provides alternate power for the DAFAS which is separate and independent from the existing PPS Power.

Testability at Power

The DAFAS design allows for the testing of the system at power. The DAFAS testing occurs at two places, in the DAFAS Cabinet and in the ARC. The test capabilities of the system are discussed in Section III.E.

Diversity from Existing Reactor Trip System

Except for the sensors, the equipment used in the design of the DAFAS is entirely diverse from the existing equipment in the PPS. The DAFAS is using a single board computer with solid state I/O Modules versus the PPS which uses Analog Bistable Trip Units to perform the same function. The DAFAS uses fiber optic technology to receive and send signals to and from its distributed I/O systems.

A common point for the DAFAS in the ARC is where the DAFAS and PPS use the same cycling and subgroup relays to control the pumps and valves in the Auxiliary Feedwater System. These relays are not used by the Reactor Trip System and their use therefore is diverse from the existing Reactor Trip System.

Electrical Independence

The DAFAS achieves electrical independence from the existing PPS by using an alternate separate power source to power the logic. The DAFAS is isolated from the ARC and Process Cabinet through the use of fiber optics. This meets the intent of the guidance for isolation from safety related circuits.

Inadvertent Actuation

The DAFAS is designed with features to minimize inadvertent actuations and challenges to the safety system. The DAFAS setpoints are set at levels that are below the existing setpoints in the PPS to prevent the possibility of the DAFAS initiating feed before the PPS during normal operation.

The DAFAS initiation relay is designed to be energized to initiate feed which is opposite the PPS which deenergizes the relays to initiate feed. This design for the DAFAS relays will prevent the loss of relay power or I/O system power from causing an inadvertent actuation as the relays are normally unpowered.

The DAFAS is blocked by the AFAS and MSIS signals to prevent DAFAS inadvertent actuations from occurring. When the PPS initiates AFAS or MSIS, indicating the PPS is operating normally and conditions for ATWS do not exist, blocking logic is activated which disables the DAFAS Relay preventing the DAFAS from controlling the feedwater flow.

The DAFAS is also blocked by the DSS such that the DAFAS will operate only when a DSS actuation has occurred.

V. SUMMARY

The system described within this report provides a compliant approach to the 10CFR50.62 Ruling. The functional requirements of the system satisfy conditions of operation and minimize the impact on current availability while lending to an achievable, installable system. Due to the numerous interactions with the NRC including requests for exemption, it is recommended that prior to implementing this or any Diverse Auxiliary Feedwater Actuation System that formal concurrence is obtained from the NRC to minimize further delays and/or modifications.

VI. REFERENCES

1. CEN-384P, "Reports to the CE Owners Group on the Design for a Diverse Emergency Feedwater Actuation System Consistent with IOCFR50.62 Guidelines", April, 1989.

2. USNRC RG 1.152, "Criteria for Programmable Digital Computer Software in Safety-Related Systems for Nuclear Power Plants".

3. ANSI/IEEE-ANS-7-4.3.2-1982, "American National Standard Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations".

4. USNRC letter, M. David Lynch to John N. Hannon, dated 8/15/89, Summary of meeting with the CEOG Regarding DEFAS Design Features to be installed per 10CFR50.62 (the ATWS Rule)

APPENDIX A

10CFR50.62 REQUIREMENTS APPLICABLE TO
COMBUSTION ENGINEERING MANUFACTURED REACTORS

"... (c) Requirements

(1) Each pressurized water reactor must have equipment from sensor output to final actuation device, that is diverse from the reactor trip system, to automatically initiate the auxiliary (or emergency) feedwater system and initiate a turbine trip under conditions indicative of an ATWS. This equipment must be designed to perform its function in a reliable manner and be independent (from sensor output to the final actuation device) from the existing reactor trip system.

(2) Each pressurized water reactor manufactured by Combustion Engineering or by Babcock and Wilcox must have a diverse scram system from the sensor output to interruption of power to the control rods. This scram system must be designed to perform its function in a reliable manner and be independent from the existing reactor trip system (from the sensor output to interruption of power to the control rods) ...

(6) Information sufficient to demonstrate to the Commission the adequacy of items in paragraph (c) (1) through (c) (5) of this section shall be submitted to the Director, Office of Nuclear Reactor Regulation.

(d) Implementation

By 180 days after the issuance of the QA guidance for non-safety related components each licensee shall develop and submit to the Director of the Office of Nuclear Reactor Regulation a proposed schedule for meeting the requirements of paragraphs (c) (1) through (c) (5) of this section. Each shall include an explanation of the schedule along with a justification if the schedule calls for final implementation later than the second refueling outage after July 26, 1984, or the date of issuance of a license authorizing operation above 5 percent of full power. A final schedule shall then be mutually agreed upon by the Commission and licensee."

10CFR50.62 GUIDANCE REGARDING SYSTEM AND EQUIPMENT SPECIFICATIONS

Guidance	Mitigating Systems
Safety Related	Not required, but the implementation must be such (IEEE-279) that the existing protection system continues to meet all applicable safety related criteria.
Redundancy	Not required.
Physical Separation from existing Reactor Trip System	Not required, unless redundant divisions and channels in the existing reactor trip system are not physically separated. The implementation must be such that separation criteria applied to the existing protection system are not violated.
Environmental Qualification	For anticipated operational occurrences only, not for accidents.
Seismic Qual.	Not required.
Quality Assurance for Test, Maintenance, and Surveillance	Explicit guidance will be issued in a letter.
Safety-Related (IE) Power Supply	Not required, but must be capable of performing safety functions with loss of off site power. Logic power must be from an instrument power supply independent from the power supplies for the existing reactor trip system. Existing RTS sensor and instrument channel power supplies may be used provided the possibility of common mode failure is prevented.
Testability at Power	Required

Guidance	Mitigating Systems
Diversity from existing Reactor common Trip	Equipment diversity to the extent reasonable and and practicable to minimize the potential for common cause failures is required from the sensors to, but not including, the final actuation device e.g., existing circuit breakers may be used for auxiliary feedwater or manufacturer. Existing protection system instrument-sensing lines may be used. Sensors and instrument-sensing lines should be selected such that adverse interactions with existing control systems are avoided.
Electrical Independence from Reactor Trip Sys.	Required up to final actuation device at which point non-safety related circuits must be isolated from Existing from safety related circuits.
Inadvertent Actuation	The design should be such that the frequency of inadvertent actuation and challenges to other safety systems is minimized.