FOR UNRESTRICTED DISTRIBUTION

DATE _____ WEC

Westinghouse Energy Systems

WESTINGHOUSE CLASS 3

WCAP-12222

ADVANCED DIGITAL FEEDWATER CONTROL SYSTEM MEDIAN SIGNAL SELECTOR FOR PACIFIC GAS & ELECTRIC CO. DIABLO CANYON UNITS 1 & 2

L. E. ERIN

MARCH, 1989

Approved: L. E. Erin for P. J. Morris
Manager,
Instrumentation and
Control Systems Licensing

Approved: for R. A. Acker
Manager,
Nuclear and Control
Technology

Approved:
Manager
Process Control Equipment

Westinghouse Electric Corporation
Power Systems Division
P. O. Box 355
Pittsburgh, Pennsylvania 15230

ABSTRACT

To improve the overall performance of the Reactor Control and Protection Systems at Diablo Canyon, the Feedwater Control System is being enhanced by the installation of a Median Signal Selector. The signal selector will eliminate a [ ]^{a,c} mechanism involving the steam generator low-low water level protective function by providing [ ]^{a,c} between the Reactor Protection System and the Feedwater Control System in accordance with the requirements of IEEE Std. 279-1971.

Various aspects of signal selector use are addressed by this report; these aspects include: 1) basis for removal of the low feedwater flow reactor trip, 2) a demonstration of the functional adequacy of the signal selection process in eliminating the [ ]^{a,c} mechanism, and 3) signal selector test and failure detection capabilities.

TABLE OF CONTENTS

Abstract
Acronyms
List of Figures

1.0 Introduction

1.1 Background
1.2 Median Signal Selector

2.0 Steam Generator Reactor Trip Functions

2.1 Steam Generator Low Low Level Reactor Trip
2.2 Low Feedwater Flow Reactor Trip

3.0 Elimination of Low Feedwater Flow Reactor Trip

3.1 Elimination via Four Steam Generator Level Channels
3.2 Elimination via Median Signal Selector
3.3 Advantages

4.0 Median Signal Selector Implementation

4.1 Operational Description
4.2 Software Description
4.3 Hardware Description

5.0 Failure Detection

5.1 Diagnostics
5.2 Test Capability

TABLE OF CONTENTS

6.0 Fault Tolerance

6.1 Reliability

6.1.1 Frequency of Failures

6.1.2 Consequences of Failures

6.1.3 Duration of Failures

6.2 Configuration Certification

7.0 Conclusion

Appendix 1 - Fault Tree for the Westinghouse EAGLE DPF Advanced Digital Feedwater Control System

ACRONYMS

RPS	Reactor Protection System
RPCS	Reactor Plant Control System
NSSS	Nuclear Steam Supply System
RCS	Reactor Coolant System
W EAGLE DPF	Westinghouse EAGLE Distributed Processing Family
I/O	Input/Output
DPU	Distributed Processing Unit
RCS	Reactor Coolant System
AFS	Auxiliary Feedwater System
FCS	Feedwater Control System
MSS	Median Signal Selector
LED	Light Emitting Diode
MTBF	Mean Time Between Failure
CLP	Control Loop Processor
AC	Alternating Current
DC	Direct Current
FSAR	Final Safety Analysis Report

LIST OF FIGURES

Figure	Title
1	Original Functional Design
2	Median Signal Selector Functional Design
3	Median Signal Selector Functional Diagram
4	Modularity Illustration
5	Westinghouse EAGLE DPF System Architecture Overview
6	Input/Output Points
7	Median Signal Selector Configuration

1.0 INTRODUCTION

1.1 Background

The fundamental purpose of plant instrumentation and control systems is to permit operational control of the Nuclear Steam Supply System (NSSS), and to initiate automatic protective action in response to unsafe operating conditions. The infrastructure of instrumentation and control systems constitutes an interactive network of electrical circuits through which protection and control functions are carried out. This network can be best described in terms of two functionally defined systems called the Reactor Protection System (RPS), and the Reactor Plant Control System. The Reactor Protection System is defined as that part of the sense and command features involved in generating those signals used primarily for reactor trip functions and the actuation of engineered safety features. The Reactor Plant Control System is defined as those electrical instrumentation and control systems that provide the operator with the necessary information and controls to effect proper primary plant control.

Accordingly, operation of a nuclear facility without undue risk to the health and safety of the public is largely predicated upon RPS design attributes which assure proper and complete operation of the RPS; these may be briefly summarized as RPS functional adequacy, and operational readiness. To insure that these characteristics are adequately implemented in the overall RPS design, the code of Federal Regulations requires that certain criteria be adhered to.

Specifically, the Code of Federal Regulations, Title 10, Part 50.55a, Codes and Standards, (h) protection systems, endorses the Institute of Electrical and Electronics Engineers Standard, IEEE-279, "Criteria for Protection Systems for Nuclear Power Generating Stations", as the governing criteria to which the Reactor Protection System design must conform, as a minimum, in order to meet the requirements of functional adequacy and operational reliability. One of the specific provisions of this standard is the issue of [

]a,c

Basically, [

]^{a,c} The mechanism may be a [physical interaction such as electrical faults originating in the control system and propagating to]^{a,c} the protection system (thereby bringing about an attendant failure within the protection system), or a [functional interaction where the action of a control system is coupled to the ability of the]^{a,c} protection system to provide adequate core protection consistent with the requirements of IEEE Std. 279-1971. Once the failure mechanism

[

]^{a,c} has occurred, the protection system must continue to satisfy all reliability, redundancy, and independence requirements. To prevent [ ]^{a,c} protection systems are, in general, designed with due regard for the requirements of physical, electrical and functional independence.

In the Westinghouse NSSS design, the Reactor Plant Control System derives many of its input signals not from dedicated control system instrument channels, but directly from the protection system instruments through isolation devices. The requirements for process parameter measurements for control and protection functions so nearly overlap that the same measurements serve both purposes equally well. Therefore, common instrument channels are, in essence, used in both the Reactor Protection System and the Reactor Plant Control System for those process parameters for which measurement is required in both the protection and control system designs. This practice allows the NSSS to be controlled from the same measurements with which it is protected. Such a scheme precludes any sensor deviation between control and protection functions which serves to maintain margins between operating conditions and safety limits thereby reducing the likelihood of spurious reactor trips, and considerably reduces the tasks of channel calibration and maintenance. However, this design configuration does present some difficulties in the area of [ ]^{a,c} and in order to take

advantage of the benefits derived from such an equipment configuration, additional measures must be taken to assure the [functional independence of the protection and control systems.]^{a,c}

1.2 Median Signal Selector

[

]^{a,c} The MSS selects the median of three steam generator narrow range level input signals [

]^{a,c}

a,c

The material in this section has been deleted from this nonproprietary document due to its proprietary nature. The material in this section discussed operational benifits and location of the Median Signal Selector.

a,c

The material in this section has been deleted from this nonproprietary document due to its proprietary nature. The material in this section discussed operational benifits and location of the Median Signal Selector.

2.0 STEAM GENERATOR REACTOR TRIP FUNCTIONS

The present Prairie Island reactor trip functions associated with the steam generator protection system are: 1) the steam generator low-low water level reactor trip and 2) the low feedwater flow reactor trip (see Figure 1).

2.1 Steam Generator Low-Low Water Level Reactor Trip

The basic function of the reactor protection circuits associated with steam generator low-low water level trip channels is to preserve the steam generator as a heat sink for removal of residual heat. This automatic protective action is taken before the steam generators are dry to maintain the heat sink, reduce the capacity and starting time requirements of the Auxiliary Feedwater System (AFS), and to minimize the thermal transient on the Reactor coolant System (RCS). This trip is actuated on coincidence of two out of three low-low water level signals in any steam generator.

2.2 Low Feedwater Flow Reactor Trip

a,c

The material in this section has been deleted from this nonproprietary document due to its proprietary nature. The material in this section discussed the low feedwater flow reactor trip.

a,c

The material in this section has been deleted from this nonproprietary document due to its proprietary nature. The material in this section discussed the low feedwater flow reactor trip.

a,c

The material in this section has been deleted from this nonproprietary document due to its proprietary nature. The material in this section discussed the low feedwater flow reactor trip.

3.0 ELIMINATION OF LOW FEEDWATER FLOW REACTOR TRIP

3.1 Elimination via Four Steam Generator Level Channels

a,c

The material in this section has been deleted from this nonproprietary document due to its proprietary nature. The material in this section discussed elimination of the low feedwater flow reactor trip via four steam generator level channels.

3.2 Elimination via Median Signal Selector

a,c

The material in this section has been deleted from this nonproprietary document due to its proprietary nature. The material in this section discussed elimination of the low feedwater flow reactor trip via a Median Signal Selector.

a,c

The material in this section has been deleted from this nonproprietary document due to its proprietary nature. The material in this section discussed elimination of the low feedwater flow reactor trip via a Median Signal Selector.

3.3 Advantages

a,c

The material in this section has been deleted from this nonproprietary document due to its proprietary nature. The material in this section discussed advantages of eliminating the low feedwater flow reactor trip.

4.0 MEDIAN SIGNAL SELECTOR IMPLEMENTATION

4.1 Operational Description

The MSS receives three isolated narrow range level input signals (see Figure 3) designated as A, B, and C for each steam generator. The algorithms are configured to [

]^{a,c,e,f} This output value is the median of the three input signals. For example, suppose that A, B, and C are signals representing 30%, 40% and 50% of steam generator level. After the [

]^{a,c,e,f} This signal representing 40% level is now forwarded to the algorithms for feedwater control. Thus, the MSS will always select the median of three input signals, [

]^{a,c}

4.2 Software Description

The Westinghouse EAGLE Distributed Processing Family (W EAGLE DPF) MSS function is configured using a Graphics Process Control Language. This high level language enables the system engineer to use menu-driven screens and interactive fill-in-the-blanks editing to configure process control loops, create a data base of input/output points and display the loops as configured during operation. The graphics language is comprised of three subsets known as Data Base Generation, Standard Modulating Control and Ladder Logic Control.

The data base of process inputs and outputs is created by using the subset called Data Base Generation. The system engineer uses an interactive editor to load the EAGLE DPF with the characteristics of each input and output point. Information such as point type (analog or digital), alarm limits, scaling and hardware address are entered into the data base for each point.

The process control loops are configured by using the Standard Modulating Control Subset. The graphics editor displays a screen showing five blank lines for input points at the top, five blank lines for output points at the bottom and eight blocks for algorithms in between (see Figure 6). The system engineer configures the control loops by filling in the blanks with input and output points defined in the data base and a standard library of 24 field proven algorithms. The inputs, algorithms and outputs are then connected to show the signal flow through the loop (see Figure 7 for MSS configuration).

In summary, the graphic process control language simplifies system configuration. This fill-in-the-blank type language affords engineering personnel the ability to make changes (if necessary in the future) without a background in computer languages such as BASIC, PASCAL, PLM86, FORTRAN, etc. The system configuration is self-documenting. All program diagrams and data base listings can be easily printed by a simple menu selection on a personal computer.

4.3 Hardware Description

The MSS function is implemented in Westinghouse EAGLE DPF equipment which is installed as part of the plant control system.

This state-of-the-art, microprocessor-based system is a mature digital design, with a history of over 280 industrial uses including utility applications. The modular features of the Westinghouse EAGLE DPF Digital Feedwater Controller with MSS permits installation into existing control cabinets, minimizing the impact on existing field terminations and wiring (see Figure 4).

EAGLE DPF utilizes a distributed architecture system and is basically comprised of input/output (I/O) cards and distributed processing units (DPU's), which contain the functional microprocessors. An overview of the EAGLE DPF system architecture is shown in Figure 5.

For the purpose of [

]^{a,c}

Power supplies for [

]^{a,c} is also provided in the Westinghouse EAGLE DPF design. Automatic [ ]^{a,c} occurs upon failure of the [ ]^{a,c}

The Westinghouse EAGLE DPF equipment represents nine years of intensive Westinghouse product development in response to a strict set of product goals. There is an extensive history of industry usage and experience to date for control system application and data acquisition.

5.0 FAILURE DETECTION

The Westinghouse EAGLE DPF MSS to be installed at Prairie Island is designed to allow for easy detection of system failures through both self diagnostics and periodic test. These methods for failure detection are discussed here below.

5.1 Diagnostics

The self-diagnostics are automatically executed during the normal operation of the system and do not disrupt the real time performance of the process. The major diagnostic features supporting the MSS function are as follows:

a,c,e,f

The material in this section has been deleted from this nonproprietary document due to its proprietary nature. The material in this section discussed the diagnostic features of the EAGLE DPF equipment.

a,c,e,f

The material in this section has been deleted from this nonproprietary document due to its proprietary nature. The material in this section discussed the diagnostic features of the EAGLE DPF equipment.

5.2 Test Capability

The MSS has been provided with the capability for on-line testing. Signal selector testing consists of [ ]^{a,c} the three steam generator level input signals and [

]^{a,c} will permit determination of whether or not the actual median signal is being chosen, and, consequently, whether the signal selector is functioning properly.

The MSS can be tested [

]a,c

6.0 SYSTEM RELIABILITY AND FAULT TOLERANCE

6.1 Reliability

From a functional stand point the implementation of a signal selector eliminates control and protection system interaction in the steam generator protection circuitry by providing functional isolation from the Feedwater Control System; however, the continued ability of the device to prevent control and protection system interaction is contingent on its ability to select the median signal. Therefore, steps have been taken to ensure the reliability of the signal selection process. Furthermore, the design provides the capability for complete unit testing that provides unambiguous determination of credible system failures.

Reliability of the Westinghouse EAGLE DPF MSS design to be installed at Diablo Canyon is focused on three major areas: minimizing the frequency of failures, minimizing the consequences of a failure, and minimizing the duration of a failure.

6.1.1 Frequency of Failures

The frequency of failures is minimized primarily by the simplification of the hardware and software design. The hardware design is based on a system organized to limit the functions and interactions of each system element. The Mean Time Between Failures (MTBF) calculation for the analog input printed circuit card is [

]^{a,b,c}

The software design is simplified by the [

]^{a,c} In addition, extensive quality assurance and testing programs are utilized to ensure an error-free system.

6.1.2 Consequences of Failures

a,c,e,f

The material in this section has been deleted from this nonproprietary document due to its proprietary nature. The material in this section discussed the consequences of failures in the EAGLE DPF equipment.

a,c,e,f

The material in this section has been deleted from this nonproprietary document due to its proprietary nature. The material in this section discussed the consequences of failures in the EAGLE DPF equipment.

[

]a,c Additionally, it should be noted that a Fault Tree for the EAGLE DPF Advanced Digital Feedwater Control System has been provided as Appendix 1 to this report.

6.1.3 Duration of Failures

The duration of a failure is minimized by the ability to diagnose and repair the system easily and quickly. For example, [

]a,c

6.2 Configuration Certification

Finally, in order to enhance the reliability of the MSS, a formal activity known as Configuration Certification has been devised to minimize design errors and provide an overall assurance that the specified functional requirements are implemented in the hardware and software as a system. Configuration Certification is accomplished via:

a,c

The material in this section has been deleted from this nonproprietary document due to its proprietary nature. The material in this section discussed configuration certification of the MSS in EAGLE DPF equipment.

7.0 CONCLUSION

Based on the information presented in this report, implementation of the Median Signal Selector function for steam generator narrow range level is evaluated to be a totally acceptable means for [

]a,c

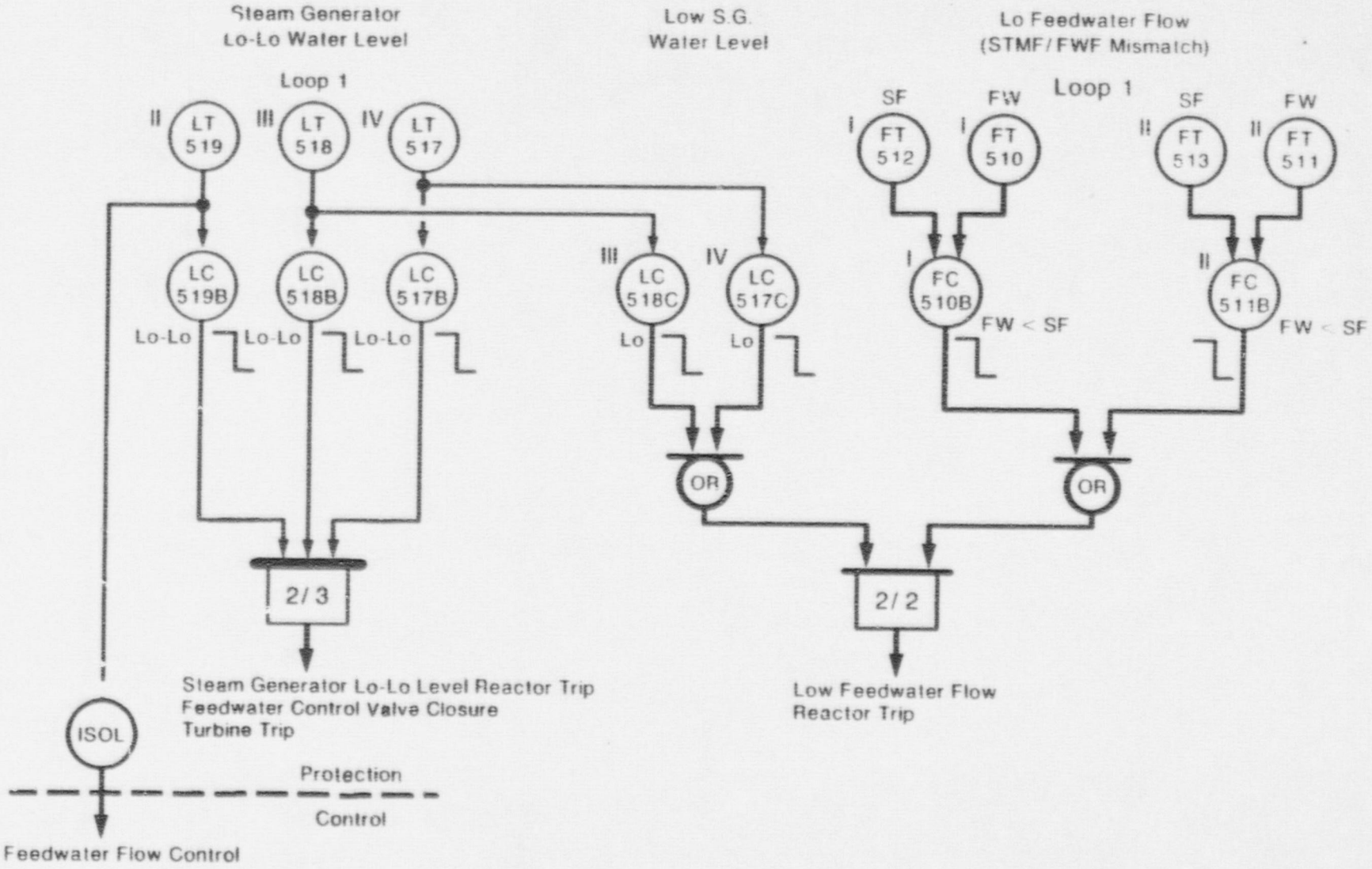
Previously, a fourth steam generator narrow range level channel has been used as an alternative to eliminate the low feedwater flow reactor trip by providing an adequate number of channels to allow for trip actuation following a [

]a,c

Finally, it should be noted that through installation of the Median Signal Selector, Diablo Canyon Units 1 and 2 will attain significant operational improvements from [

]a,c reduced fatigue buildup on critical components, and improved Feedwater Control System reliability. Futhermore, the MSS function is easily accomplished in conjunction with the Diablo Canyon Feedwater Control System upgrade which utilizes the Eagle DPF equipment.

FIGURE 1 - ORIGINAL FUNCTIONAL DESIGN



1366 D28908.001

FIGURE 2
MEDIAN SIGNAL SELECTOR FUNCTIONAL DESIGN a,c,e,

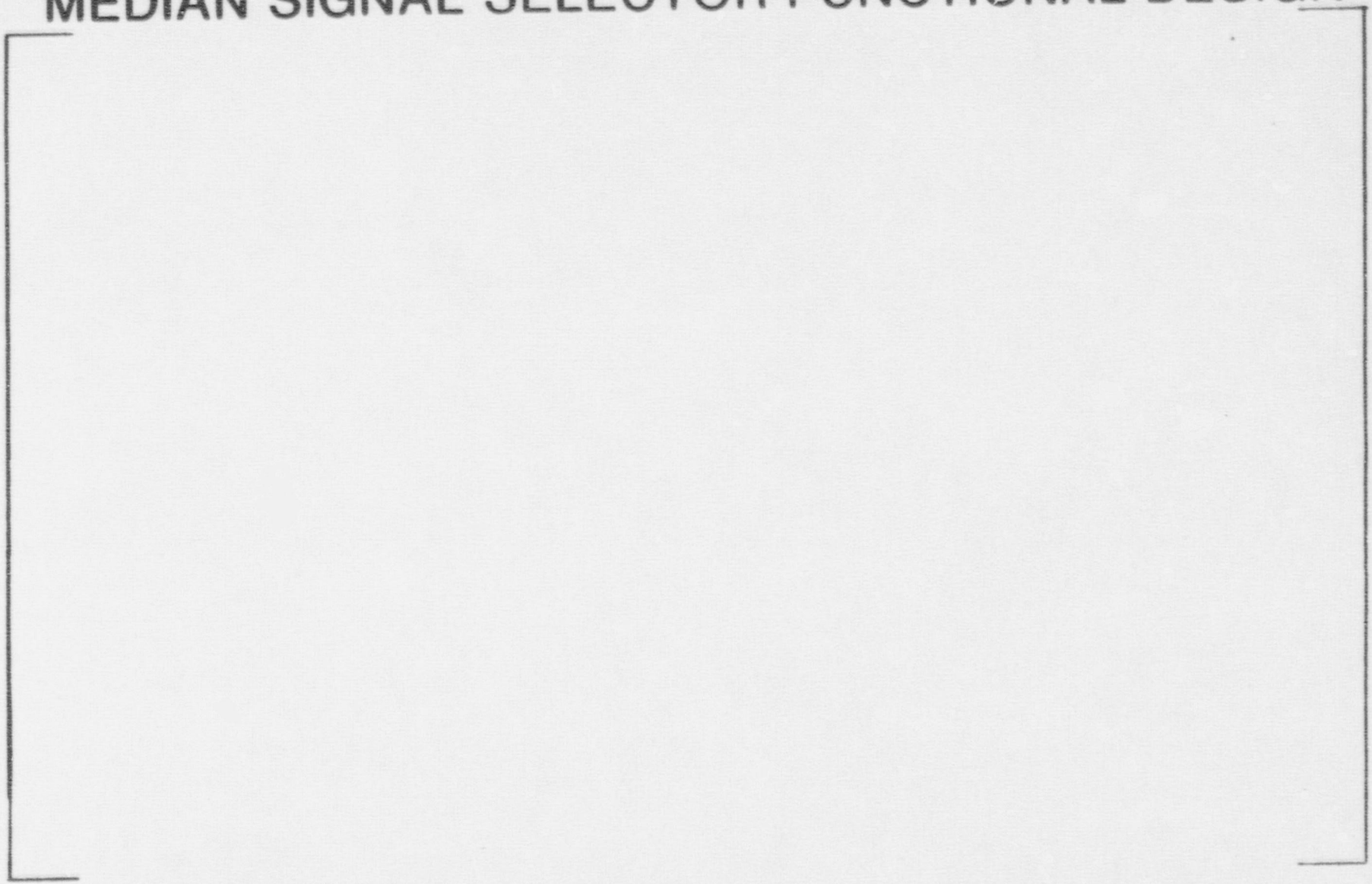
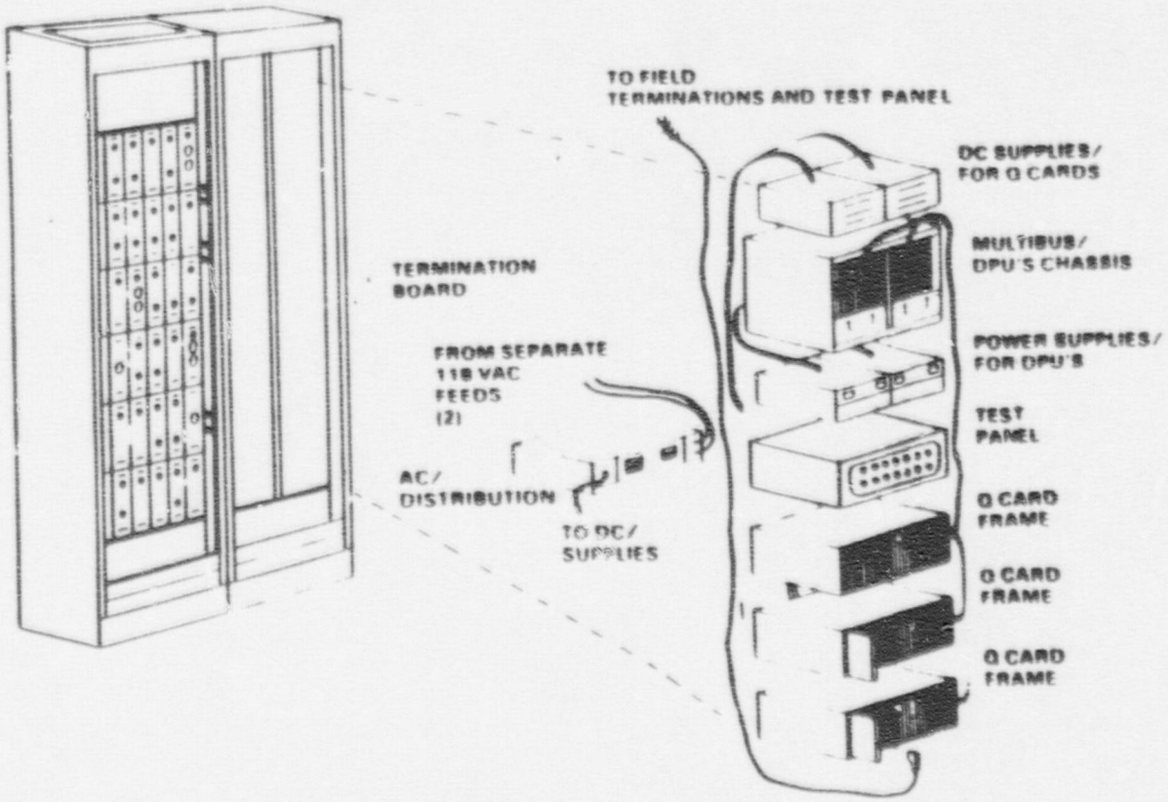


FIGURE 3
MEDIAN SIGNAL SELECTOR - FUNCTIONAL DIAGRAM [a,c,e,f]

FIGURE 4 - MODULARITY ILLUSTRATION

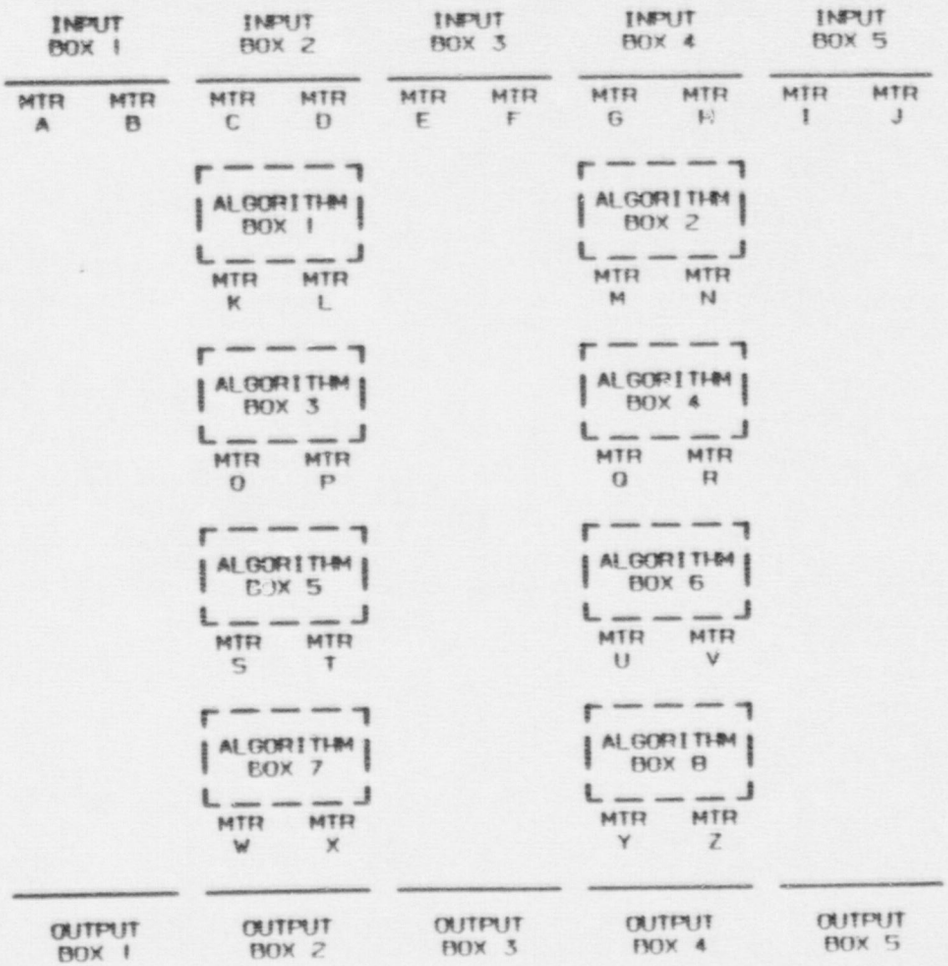


1328 D26228 001 P/B

FIGURE 5 - WESTINGHOUSE EAGLE DPF SYSTEM ARCHITECTURE OVERVIEW

a,c,e,f

FIGURE 6 - INPUT/OUTPUT POINTS



1328 D26228.003 P/B

FIGURE 7
MEDIAN SIGNAL SELECTOR CONFIGURATION a,c,e,f

APPENDIX 1

FAULT TREE FOR THE WESTINGHOUSE EAGLE DPF
ADVANCED DIGITAL FEEDWATER CONTROL SYSTEM

a,c

The material in this section has been deleted from this nonproprietary document due to its proprietary nature. This section discussed the fault tree for the Westinghouse EAGLE DPF Advanced Digital Feedwater Control System.

FAULT TREE FOR EAGLE DPF ADVANCED DIGITAL FEEDWATER CONTROL SYSTEM a,c