Westinghouse Energy Systems

Westinghouse Energy Systems

WESTINGHOUSE CLASS 3

WCAP-12676

MEDIAN SIGNAL SELECTOR FOR WESTINGHOUSE 7300 SERIES PROCESS INSTRUMENTATION

APPLICATION TO WESTINGHOUSE THREE LOOP PLANTS EMPLOYING THE RTD BYPASS ELIMINATION ALABAMA LIGHT COMPANY JOSEPH M. FARLEY UNIT 1

J. F. Mermigos
July 1990

Reviewed By: ______________
Instrumentation and
Control Systems Licensing

Approved: ______________
Manager,
Instrumentation and
Control Systems Licensing

Westinghouse Electric Corporation
Energy Systems
P. O. Box 355
Pittsburgh, PA 15230

ABSTRACT

To maintain the current level of functional performance of the Reactor Protection System subsequent to implementation of the resistance temperature detector bypass elimination (RTDBE) design modification at the Beaver Valley Unit 2 Nuclear Station, the existing Reactor Control System must be modified by installation of a Median Signal Selector. The signal selector will prevent a potential control and protection system interaction mechanism involving the thermal overpower and overtemperature protective functions by providing [ ][a,c] between the Reactor Protection System and the Reactor Control System, in accordance with the requirements of IEEE Standard 279-1971, Section 4.7.

Various aspects of signal selector use are addressed by this report; these aspects include a demonstration of the functional adequacy of the signal selection process in preventing the interaction mechanism, requirements regarding device reliability such as signal selector test and failure detection capabilities, and the Median Signal Selector's [ ][a,c] Additionally, recommendations regarding actions on the part of the operator necessary to support signal selector use are presented.

TABLE OF CONTENTS

LIST OF FIGURES

ACRONYMS

MTBF - Mean Time Before Failure

RTD - Resistance Temperature Detector

RTDBE - Resistance Temperature Detector Bypass Elimination

T-avg - Average Temperature

RCS - Reactor Coolant System

SECTION 1.0
INTRODUCTION

In order to implement the resistance temperature detector bypass elimination (RTDBE) design modification at the Joseph M. Farley Unit 1 Nuclear Station, certain configurational changes must be made to the existing plant instrumentation and control complex to assure that the functional capability and inherent reliability provided in the original Reactor Protection System design are not compromised. Consequently, to preserve these characteristics, a Median Signal Selector is implemented in the Reactor Control System for receiving reactor coolant temperature information. The function of the signal selector is to eliminate the potential for a control and protection system interaction mechanism involving the Reactor Control System and the thermal overpower and overtemperature protective functions in accordance with the requirements of The Institute of Electrical and Electronics Engineers Standard, IEEE Standard 279-1971, "Criteria for Protection Systems for Nuclear Powered Generating Stations", Section 4.7.

The following report constitutes the technical basis upon which the application of a signal selection device to the integrated RTDBE design is justified. Various aspects of signal selector use are addressed by this report; these aspects include a demonstration of the sufficiency of the signal selection process in eliminating the interaction mechanism, and requirements regarding device reliability such as signal selector test and failure detection capabilities. Additionally, recommendations regarding actions on the part of the utility necessary to support signal selector use are provided.

1.1 BACKGROUND

The fundamental purpose of plant instrumentation and control systems is to permit control of nuclear plant operations, 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, and the Reactor 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 Control Systems are defined as those electrical instrumentation and control systems that provide the operator with the necessary information and controls to affect proper primary plant control.

IEEE Standard 279-1971 is the governing criteria to which the Reactor Protection System design must conform, as a minimum, in order to meet the degree of operational reliability and functional adequacy considered acceptable for nuclear plant service. One of the specific provisions of this standard is the issue of control and protection system interaction as presented in Section 4.7.

Control and protection system interaction addresses any mechanism whereby the ability of the protection system to accomplish its safety related function is adversely affected by nonsafety related plant control systems. The mechanism may be a physical interaction such as electrical faults originating from within the control system and propagating to the Reactor Protection System (thereby bringing about an attendant failure within the protection system), or a functional interaction whereby the action of a control system degrades the ability of the protection system to provide adequate core protection consistent with the requirements of IEEE Standard 279-1971. To prevent control and protection system interactions, protection systems are, in general, designed with due regard for the requirements of physical, electrical and functional independence relative to non-protection (control) systems.

1.2 APPLICATION TO THE RTDBE MODIFICATION

The current temperature measurement instrumentation provided for Westinghouse three loop plants consists of two separate and distinct sets of instrument channels. One set is designated as a Class-1E system, and constitutes a portion of the Reactor Protection System. It is utilized to provide reactor coolant temperature information to the RPS for the generation of thermal overpower and overtemperature protective functions. The other set is non Class-1E, control grade equipment that supplies temperature information required by the plant control systems for proper primary plant control.

With the implementation of the RTDBE modification, the dedicated control system resistance temperature detector (RTD) elements will be eliminated. Therefore, temperature signals for use in the plant control systems must now be derived from the protection system RTDs. As a result of this configuration change, new complexities regarding control and protection system interaction are introduced into the process system design. Consequently, additional measures must be taken to assure the functional independence of the protection and control systems. To eliminate any degrading control and protection system interaction mechanisms introduced as a result of the RTDBE modification, a Median Signal Selector has been incorporated into the Reactor Control System design. The Median Signal Selector preserves the [ ]^{a,c} of interfacing control and protection systems that share common instrument channels.

Protective functions associated with the temperature measurement instrumentation consist of two reactor trip channels; the overpower delta-T trip channel and the overtemperature delta-T trip channel. These protective functions utilize loop T-avg and delta-T signals, derived from the RCS loop narrow range T-hot and T-cold measurements, to provide core protection against several Condition II accidents as detailed in the plant's Safety Analysis Report. Both of these trips are configured with two out of three (2/3) actuation logic. The logic scheme is depicted in Figure 1, Functional Logic Diagram for Reactor Trip Functions.

Because the dedicated control system RTD elements will be eliminated by the RTDBE modification, it is necessary to supply temperature information to the Reactor Control System from the protection system. For the RTDBE implementation, the calculated temperature signals T-avg and delta-T (one signal per loop) are supplied as input to the Reactor Control System. Thus, proper operation of the Reactor Control System will be dependent on the integrity of the channel selected. This characteristic imparts a functional dependence of the Reactor Control System on the Reactor Protection System. This introduces the possibility that certain failures, which may occur in the Reactor Protection System, may negate a particular channel of a protective function, and simultaneously cause undesirable control system action that requires subsequent protective action, from the failed safety function, in order to prevent the transient from exceeding any design safety limits. For such a scenario, IEEE Standard 279-1971, Section 4.7.3 imposes the consideration of an <u>additional</u> random failure in the Reactor Protection System.

The underlying logic is that the initial protection system failure is considered the initiating event for the transient and, therefore, does not constitute the "single failure" IEEE Standard 279-1971 imposes on the protection system. As such, an additional protection system failure must be postulated to occur, and the protection system must continue to be capable of initiating the appropriate protective action.

For example, consider the hypothetical situation where a single T-avg protection signal is utilized to provide the input to the Reactor Control System. Failure of this temperature channel in the low direction will generate control system action that results in control rod withdrawal. Consequently, the thermal overpower and overtemperature protection channels may be subsequently required. The limiting single failure in this instance would be a failure of one of the two <u>remaining</u> T-avg temperature channels. This leaves only one operable channel which is insufficient to satisfy the 2/3 actuation logic implemented in the overpower and overtemperature reactor trip functions.

One solution to this problem is to eliminate the need to consider a second random failure by functionally isolating the Reactor Control System from the Reactor Protection System. This is accomplished by implementing a Median Signal Selector in the Reactor Control System. The signal selector will receive as input all three channels of T-avg information, and choose the median signal for control purposes. Thus any single failed temperature channel will not result in adverse control system behavior. The delta-T signals that are transmitted to the control system are not required to be input to a Median Signal Selector since there are no control and protection system interactions associated with the delta-T calculated signal. Although the delta-T signals can be input to improve the availability of the delta-T calculated signal. A block diagram illustrating the protection system inputs to the control system is shown in Figure 2. The control and protection systems are then functionally isolated, as well as physically and electrically isolated. Thus, T-avg signals resulting from a single failed high or low temperature channel will be rejected for control purposes and, therefore, will not affect the plant control system. Hence, the control and protection system interaction mechanism has been eliminated.

SECTION 2.0
SIGNAL SELECTOR IMPLEMENTATION

The objective of this report is to address engineering issues relative to the use of a Median Signal Selector in eliminating control and protection system interaction involving the Reactor Control System. In meeting this objective, the characteristics of signal selector operation and signal selector reliability will be developed. The discussion regarding signal selector operation describes the units hardware configuration and evinces the operating principal of the signal selector. This demonstrates how the device provides functional isolation as detailed in Section 1. The discussion regarding signal selector reliability demonstrates that the signal selector possesses the requisite degree of operational readiness acceptable for nuclear plant service. This discussion will address quality of signal selector hardware, and the capability for, and adequacy of signal selector testing.

2.1 SIGNAL SELECTOR OPERATION AND CONFIGURATION

a,c

The information in this section has been omitted from the non-proprietary version due to its proprietary nature. This section dealt with Signal Selector Operation and Configuration

The Median Signal Selector (MSS) for the process instrumentation at the Joseph M. Farley Unit 1 Nuclear Station consists of four auctioneers. (The four auctioneers are NSA G03 and NSA G04 modules, for low select, and high select, respectively.) There are three low select auctioneers and one high select auctioneer. Another card (NTP module) is required to provide test points. The four active cards consist of operational amplifiers configured with appropriate input and feedback resistance and diode networks and with appropriate input and output signal conditioning. The algorithm of this system produces an output signal that is equal (in voltage) to the median of the three input signals.

To develop this algorithm one starts by using the three low select auctioneers. For a block diagram layout of the Median Signal Selector see Figure 3, SIGNAL SELECTOR BLOCK DIAGRAM. Into these three low select auctioneers are input all combinations of the three input signals in groups of two. For example, Low Auctioneer 1 would have as its inputs signals A and B. Low Auctioneer 2 would have signals B and C and Low Auctioneer 3 would have A and C. This "first stage" of the signal selector process will eliminate the highest of all three signals.

The next step of the median signal selector process uses the High Select Auctioneer. The output of the three low auctioneering cards will be input to the high auctioneer. The inputs to this high auctioneer will be the median signal and two signals that are the lowest signal. The high select will choose the highest of these three signals which will be the median signal of the three original input signals. The "first stage" of the signal selector eliminated the highest signal, and the "second stage" of the signal selector eliminated the lowest of the input signals.

We have illustrated how the median signal selector rejects signals that are lower or higher than the median. In normal operation the low and high signals will be within the accuracy tolerance. In the case that a signal should be low or high because it has failed, i.e., it has failed to achieve the accuracy tolerance, we have demonstrated how it is rejected for control purposes. In other words, the control and protection interaction mechanism has been eliminated, in that a single failed protection signal will not be propagated into the control system.

2.2 SIGNAL SELECTOR RELIABILITY

a,c

The information in this section has been omitted from the non-proprietary version due to its proprietary nature. This section dealt with Signal Selector Reliability

[

]a,c Therefore, steps have been taken to ensure the reliability of the signal selection process. [

]a,c

The key to ensuring proper signal selector operation lies with the unit's reliability. The signal selector is designed to be consistent with the reliability characteristics necessary to preserve the total integrity of the protection system.

[

]a,c

[

]a,c

IEEE Standard 279-1971 delineates certain functional performance requirements regarding aspects of system reliability for protection systems. Because the signal selector will be implemented to support the protection system, it has been evaluated against those criteria considered applicable to its design as presented below.

Capability for Unit Test:

The signal selector has been provided with the capability for on line testing. Signal selector testing consists of monitoring the three input signals and the one output signal via test points. Comparison of the output signal to the input signals permit determination of whether or not the median signal is being passed, and, consequently, whether the signal selector is functioning properly. Any output signal at a value other than that corresponding to the median signal is indicative of a unit failure.

The signal selector should be tested concurrently with the protection instrument channels feeding the unit. Test signals are received from the protection system, as would a normal process signal, when the individual instrument channels are placed in the test mode. [

]a,c As the test signal magnitude is varied, that instrument channel which represents the median signal will also be altered allowing the technician to determine the presence of proper signal selector action.

Signal selector testing consists of measuring input and output signals which allow the operator to infer proper unit operation. We may examine, in principal, a typical test sequence for the signal selector. As an example consider the following assignments of hypothethical signal strengths to the three instrument channels feeding the signal selector.

Channel A - 4.0 volts
Channel B - 5.0 volts
Channel C - 6.0 volts

With these assignments, Channel B would be selected as the median signal. This may be verified by noting the signal selector output voltage at the appropriate test point. Now, let channel A be taken to test. As the signal strength of Channel A is adjusted to any value less than 5.0 volts, channel B will continue to be selected as the median signal. However, as the test signal strength is adjusted to a value between 5.0 and 6.0 volts, channel A (the test channel) should be selected as the median signal, and finally as the test signal is raised to a value in excess of 6.0 volts, channel C will be selected.

In this manner, testing with a single input channel permits an assessment of a spectrum of signal selector operational modes. Furthermore, it should be emphasized that although each operational amplifier in the circuit is not specifically exercised during testing of an individual channel, all operational amplifiers will have been exercised once each of the three protection sets has been tested. [

][a,c]

It should also be noted that in practice, during normal operation, instrumentation channel signal strengths may be sufficiently close that their degree of proximity to one another makes it difficult (if not impossible) to determine when the test channel signal falls between the remaining two channels. Nevertheless, it is still possible to determine proper signal selector operation by verifying that the test channel is indeed rejected when it is taken to the high or low position.

Quality of Components:

Components utilized in the signal selector are of a quality consistent with low failure rates and minimum maintenance requirements, and conform to protection system requirements. [

Equipment Qualification:

Equipment qualification is aimed at improving the operational reliability of safety related equipment by reducing the potential for common mode failures brought about by adverse environmental influences. [

]^{a,c}

The remaining attributes of IEEE Standard 279-1971, Section 4 are not considered applicable to the signal selector design.

2.3 FAILURE DETECTION

At this point it is instructive to illustrate how system failures will manifest themselves at the signal selector output; in doing so, we further justify the test capabilities of the signal selector as being adequate for failure detection.

Let the previous signal assignment apply with Channel A in test. As channel A is varied, all four modules are exercised. Not all components in modules are exercised, however. For example the low auctioneer may be passing a low signal and if the test voltage is higher, then the output of that module is not changing. However, it must be operational for proper device action. One may postulate the failure of any active component, (the buffer amplifier corresponding to the B input to the low auctioneer, for example) such that it passes a voltage signal magnitude other than the magnitude received from the protection system, which for our purposes is 5.0 volts as determined by direct measurement at the output. With the test signal (channel A) adjust to any value that forces the "selection" of channel B as the median signal, the output of the MSS should be of equal magnitude as the input to B (5.0 volts). However, the input buffer in B has been failed by postulate to some value other than 5.0 volts which has an attendant effect on the signal selector output voltage; therefore, the signal selector output voltage will reflect this anomaly and signal selector failure is detected.

Similar scenarios may be postulated for each of the other amplifiers with equally unambiguous results. In fact the following generalities regarding failure modes may be stated:

1. Failure of any single amplifier in the auctioneering circuits will be readily manifest through test point voltage measurements alone, if it forces the auctioneer to pass a voltage different from the expected voltage based on measurement of the actual protection system input signals.

2. Failure of any single amplifier in the auctioneer circuit that does not force the above action (such as a failure of the highest reading amplifier in the low auctioneer circuit failing high) will be apparent during test once the test voltage is adjusted to a value which would, under normal conditions, force the failed amplifier's signal to be passed, as determined by examination of the input voltages.

   Inasmuch as all modules will be exercised during a complete test sequence, even "as-is" failures, in which an amplifier fails at an output voltage which corresponds to its output under normal operating conditions, will be readily detected as the test procedure is conducted. Multiple failures in the MSS will simply compound the effects of failure. Of course, in practice, it is not necessary to determine to which amplifier the failure is confined; rather, a simple card replacement followed by a repeat test sequence will reveal correction of any problems that have been identified. Thus, we find that rot only is the signal selector design consistent with low failure probability, but that circuit failures are clearly manifest during MSS testing.

2.4 FAULT CONDITIONS FROM 7300 FAILURES

a,c

[

The information in this section has been deleted from the non-proprietary version due to its proprietary nature. This section dealt with Fault Conditions From 7300 Failures

]

The following assumptions were made in evaluating the 7300 fault outputs.

1. A failure on the non-Class 1E side was considered the same as a control failure. [

]a,c

2. [

]a,c It was not assumed that the isolation device prevents the failure from propagating across to the non-Class 1E side.

3. The analysis was limited to a single failure. Multiple failures on the same board/channel were not considered.

4. Failures that caused the output to remain "as-is" were considered acceptable.

<u>RESULTS</u>

a,c

[

]

2.5 RECOMMENDED OPERATOR ACTIONS

The objective of this report is to present information which supports the implementation of a signal selection device as part of the RTDBE design modification. A properly designed selection unit, that possesses the requisite reliability characteristics as presented earlier, is paramount to preserving the total integrity of the Reactor Protection System. Notwithstanding, signal selector implementation must be fully integrated into the overall plant operating scheme. Consequently, certain actions and policies need to be adapted by the utility in order to preserve the integrity of the Reactor Protection System. These actions include:

1. Conducting a review of all pertinent operating procedures to ensure they are consistent with, and support operation with a signal selector, including administrative controls for operations with the signal selector disabled, or in a test mode. For example, when performing functional checks the protection channel should be in the tripped condition. Attendant procedura modification should be affected.

2. Implementing necessary administrative controls to ensure that signal selector testing is carried out at the appropriate frequency, and that consistent requirements for control room surveillance of Reactor Coolant System temperature during the shift are established.

3. Developing procedures for signal selector testing including test acceptance criteria.

SECTION 3.0
CONCLUSION

Based on the information presented in this document, a Median Signal Selector is deemed an acceptable means of addressing control and protection system interaction following the implementation of the RTD Bypass Elimination modification. Whereas the signal selector is being utilized to address an aspect of protection system functional performance relative to IEEE Standard 279-1971, [

]a,c

Additionally, high quality components commensurate with those used in the protection system are also used to improve the overall unit reliability. Due consideration of the "Recommended Operator Actions" presented in Section 2.4 is essential to the application of the signal selector in preserving the total protection system integrity.

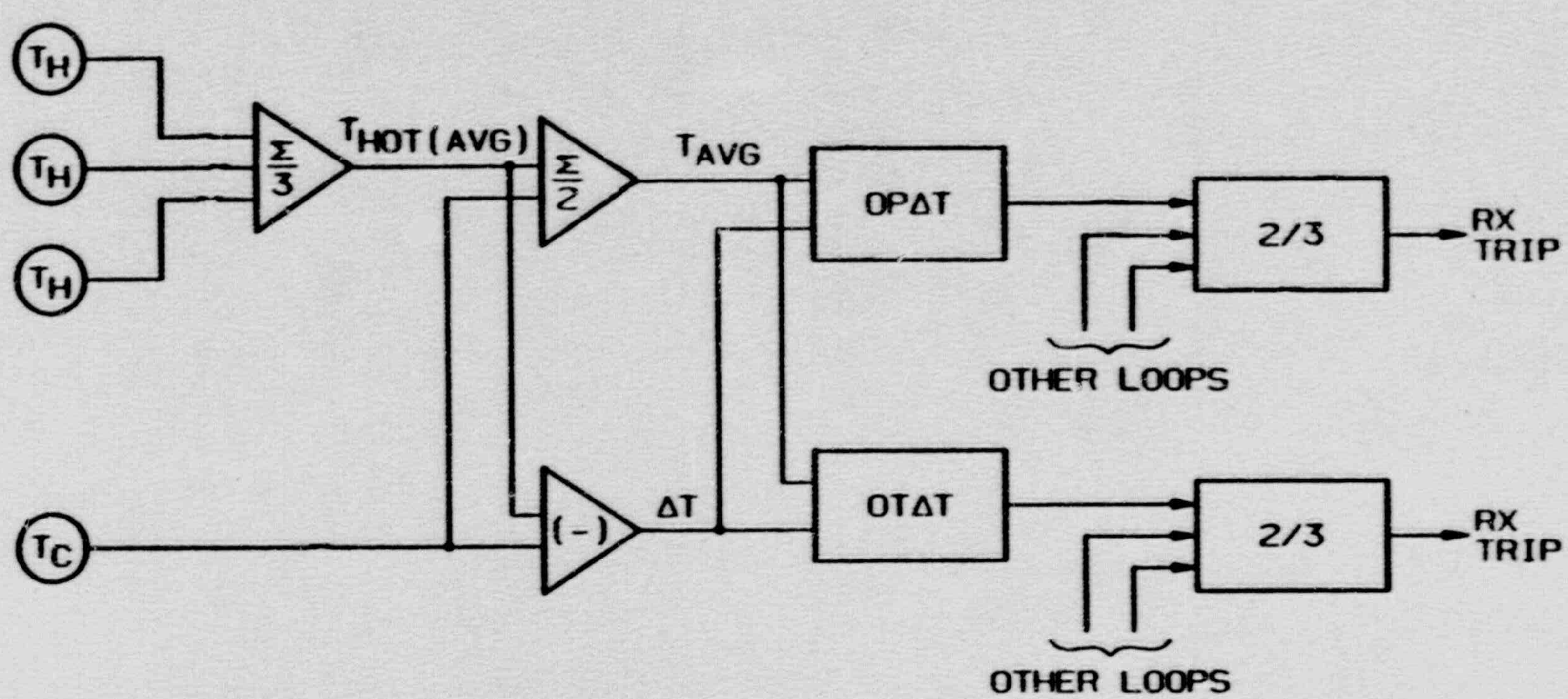

FIGURE 1: Reactor Thermal Overpower & Overtemperature Protection Functional Diagram

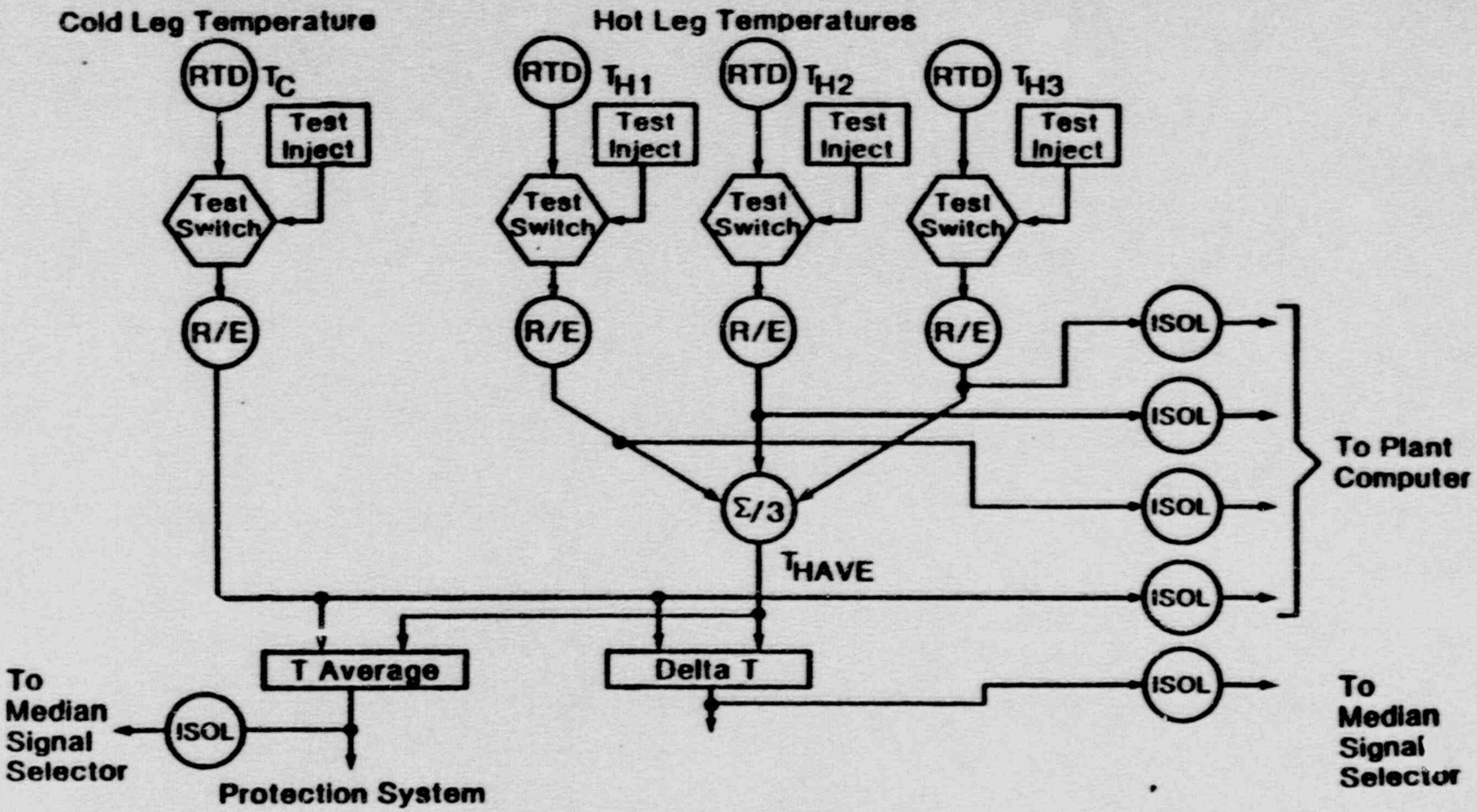

FIGURE 2: Protection System Inputs to Control System

D0176:1D-031590

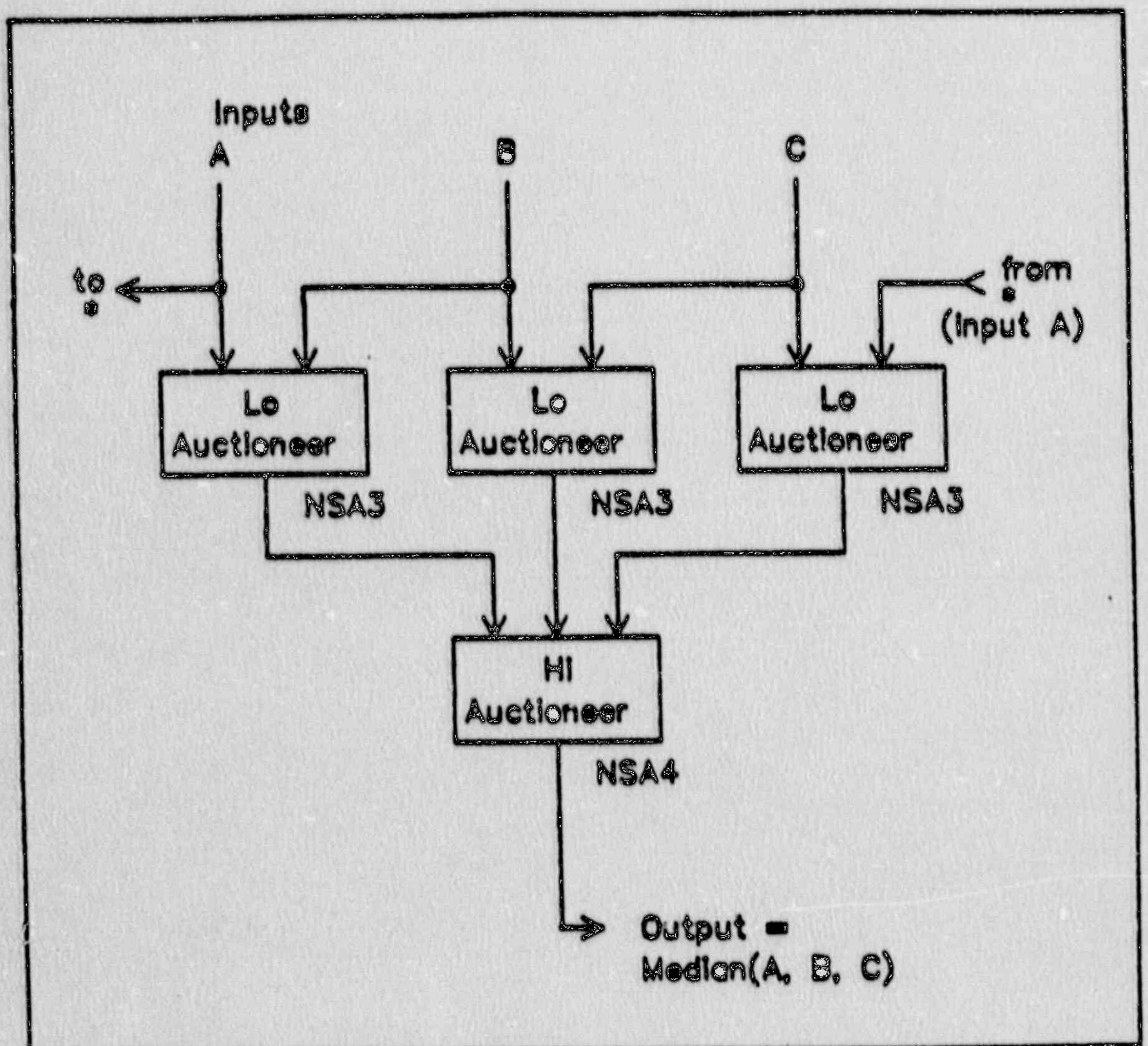

FIGURE 3

SIGNAL SELECTOR BLOCK DIAGRAM