Westinghouse Technology Systems Manual

Section 12.1

Reactor Protection System

TABLE OF CONTENTS

LIST OF FIGURES

12.1 REACTOR PROTECTION SYSTEM

Learning Objectives:

1. State the purposes of the Reactor Protection System (RPS).

2. Explain how the following design features are incorporated into the RPS:

    a. Single failure criterion,
    b. Testability,
    c. Equipment qualification,
    d. Independence,
    e. Diversity, and
    f. Prevention of control and protection system interaction.

3. Describe the sequence of events (flowpath) beginning at the sensor up to and including the starting of an Engineered Safety Feature (ESF) component and/or the opening of a reactor trip breaker.

4. Explain how failures in the rod control system are prevented from affecting reactor trip capability.

12.1.1 Introduction

The purposes of the reactor protection system are as follows:

1. To initiate a reactor trip if safe operating limits are exceeded, and
2. To initiate engineered safety features actuation(s) if an accident occurs.

The overall purpose of the reactor protection system is to prevent the release of radioactivity to the environment. To meet this objective, the RPS acts to prevent the unsafe operation of the reactor. The initiation of a reactor trip by the RPS prevents the core from operating in a condition that could cause damage to the core. Also, if an accident occurs, the RPS trips the reactor and actuates the engineered safety features. These safety features mitigate the consequences of the accident.

The reactor plant operating limits are determined and set by the utility's Final Safety Analysis Report (FSAR). The plant incorporates these limits into its technical specifications, and the NRC appends the technical specifications to the plant's operating license. To keep plant conditions within these operating limits, local sensors monitor various processes; these sensors are capable of detecting a condition that would require a reactor trip or an engineered safety features actuation.

Bistables in the analog circuitry (located within the analog cabinets) compare analog input signals, supplied by process sensors, to preselected trip or actuation setpoints. If a process signal exceeds a setpoint, the output of the associated bistable is changed. The bistable thus converts the analog signal into a digital output (on or off, energized or de-energized) which is monitored by the trip logic matrix. Based on

the status of the inputs from the bistables, the logic matrices (located within the logic cabinets) determine whether the RPS should generate a reactor trip or initiate an engineered safety features actuation.

12.1.2 System Description

12.1.2.1 Reactor Protection System Design

To guarantee the integrity of the reactor and to avoid an undue risk to the public health and safety, the plant design incorporates a reactor protection system. This system is capable of supplying reactor and component trip signals and initiates the engineered safety features, which provide protection for normal operating, transient, and accident conditions.

The reactor protection system contains two complete and independent trains of analog and logic circuits. If an analog circuit senses an unsafe condition, signals are sent to the protection system logic cabinets, where the appropriate logic contacts open. The logic matrices (circuits) determine whether the coincidence for a reactor trip function is satisfied. If so, the protection system opens the reactor trip breakers. Opening these breakers removes power from the control rod drive mechanisms, allowing the rods to fall into the reactor core. If an accident occurs and an engineered safety features actuation is required, the protection system actuates the appropriate safety equipment. In addition, the logic trains automatically enable or remove permissives (protection-grade interlocks).

12.1.2.2 Compliance with General Design Criteria (GDC)

The reactor protection system designed by Westinghouse meets the General Design Criteria of 10 CFR Part 50. In addition, the protection system complies with various Regulatory Guides and several different IEEE Standards. These documents include:

1. “General Design Criteria for Nuclear Power Plants,” Appendix A to Title 10 CFR 50,
2. United States Nuclear Regulatory Commission Regulatory Guides,
3. “Criteria for Protection Systems for Nuclear Power Generating Stations,” IEEE 279-1971,
4. “Criteria for Class 1E Electrical Systems for Nuclear Power Generating Stations,” IEEE 308-1971, and
5. “Trial-Use Criteria for Periodic Testing of Nuclear Power Generating Station Protection Systems,” IEEE 338-1971.

12.1.2.3 Single-Failure Criterion

The reactor protection system contains redundant instrumentation channels (two to four instruments) for each protective function. These process instruments provide signals to a one-out-of-two logic train scheme and are electrically isolated and physically separated from each other. Either logic train sensing the required coincidence can provide the required protective actions (either a reactor trip or an

engineered safety features actuation). Any single failure within a channel or train does not prevent a protective action when required. The RPS is testable, with the reactor operating, without reducing its reliability of operation. These features meet the requirements of General Design Criteria 21 and 22 and Regulatory Guide 1.53. A loss of input power (the most likely mode of failure) to the protection system results in the system failing to a safe state or into a state demonstrated to be acceptable. This feature meets the requirements of GDC 23.

12.1.2.4 Testability

The RPS is testable during all plant conditions. The RPS is tested in a segmented fashion, in which each test section overlaps an adjacent test section. Such testing ensures both the availability and the accuracy of the system from the process sensors to the final devices (trip breakers, ESF equipment, etc.).

12.1.2.5 Equipment Qualification

Following an accident, a loss-of-coolant accident (LOCA) or some other high energy line break, the environmental conditions inside the containment degrade (i.e., temperature, pressure and radiation levels increase). All safety systems, components and instruments important to safety must remain functional in order to provide their intended safety functions. Therefore, a wide range of environmental qualification tests and functional performance tests is employed to ensure equipment survivability. These test results demonstrate that the safety equipment meets the requirements of GDC 22.

12.1.2.6 Independence

Each process instrument is assigned to one of the four protection channels (Channels I, II, III, and IV). Channel independence is maintained throughout the system. This independence extends from the sensor to the device which actuates the protective function. Physical separation is used to achieve separation of redundant transmitters. Separation of wiring is achieved by using separate wireways, cable trays, conduit runs, and containment penetrations for redundant channels. Redundant analog equipment is separated by locating modules in different protection racks. Finally, each redundant channel is powered from a separate vital ac power source. These features meet the requirements of GDC 22.

There are two reactor trip breakers, each of which is automatically opened (tripped) by its own dedicated logic matrix. The series-connected reactor trip breakers supply power to the rod drive mechanisms. Opening either breaker interrupts power to all rod drive mechanisms, allowing the rods to fall freely into the core.

12.1.2.7 Diversity

To ensure the safe operation of the reactor core and to protect the reactor coolant system pressure boundary, the RPS continuously monitors numerous diverse process system variables. The extent of this diversity has been evaluated for a great number of postulated accidents. Generally, one or more diverse protection functions would generate a reactor trip or mitigate an accident before intolerable

consequences could occur. This feature meets the requirements of GDC 21 and GDC 22.

12.1.2.8 Control and Protection System Interaction

The reactor protection system is designed to be independent of all process control systems. However, in certain applications, some control signals and other nonprotective functions are derived from individual protection channels through isolation amplifiers. The isolation amplifiers are classified as part of the protection system and are most often located within the reactor protection analog racks. The isolation amplifier is designed so that a short circuit or open circuit in, or a voltage (ac or dc) applied to, the isolated output portion of the amplifier (the control side of the circuit) does not affect the input (protective) side of the circuit. Any signal passed through an isolation amplifier is never returned to the protection racks. This feature meets the requirements of GDC 24.

If the failure of a protection system process instrument or component causes a plant transient which requires a protective action (e.g., a reactor trip), the protection system is designed to withstand another, independent failure without the loss of the protective function.

12.1.3 Component Descriptions

The Westinghouse protection system may be one of several different designs. The common designs are the relay protection system and the solid-state protection system. Either of these systems performs the same functions as stated in the system description, with the solid-state protection system being a more recent design. Descriptions of both systems are included, with specific differences explained. This section also provides descriptions of the reactor trip breakers and their protection system interfaces.

Some facilities have upgraded portions of their solid-state protection systems to the Eagle-21 protection system sold by Westinghouse. This section does not discuss the Eagle-21 system. The innovative feature of the Eagle-21 system is that it is an on-line, self-testing protection system. Using solid-state devices, this system checks the entire protection system regardless of the operational condition of the reactor, and it performs these functional tests continuously.

12.1.3.1 Relay Protection System

The relay protection system is explained by describing the features shown on Figure 12.1-1.

1. Red, White, Blue, Yellow - Redundant analog protection channels originate at the process sensors. Each channel is powered from an independent vital power supply.

2. Isolation Amplifier - The control systems are separate and distinct from the protection system. The control systems are, however, dependent upon signals derived from the protection system through these isolation amplifiers.

3. External Signal Input - The signal conditioning equipment of each protection channel in service during normal operations is capable of being calibrated and tested independently. This is accomplished by inserting analog signals to verify proper operation without tripping the reactor. This allows testing throughout the channel to the protection bistable output.

4. Channel Test Switch – This switch provides the path for the application of an external signal input to the protection bistable, and it also provides a path to an alarm which alerts the operator that the proper testing sequence has not been followed (see item 6 below).

5. Protection Bistable – The bistable is an electronic switch with an adjustable on-off setpoint. It is designed to interrupt control power to both the train A and train B logic cabinet input relays.

   Within the bistable, a signal from the process sensor is compared to a preset, adjustable setpoint. When the process signal equals or exceeds the setpoint value, the bistable's output is turned off (de-energized), and its output voltage goes to zero (the bistable is tripped). This electronic device or switch thus converts the analog (variable) input signal into a digital (on-off) output signal. The input relays (item 7 below) of the logic cabinet receive this digital signal.

6. Bistable Output Trip Switch – This switch permits verification of the bistable's operability by providing continuity through the "Proving Lamp." When this switch is placed in the trip position, the bistable's output is no longer connected to the logic matrices. To the logic matrices, removing the bistable's output by placing the bistable output trip switch in trip is indistinguishable from the bistable actually tripping as described in item 5 above. Hence, placing the output trip switch in trip is somewhat confusingly referred to as "tripping the bistable."

   With the switch in trip, the technician varies a test input signal via a signal generator as described in items 3 and 4 above. When the test signal equals the trip setpoint, the bistable trips (the output is de-energized), and so the proving lamp de-energizes. This process provides verification of the bistable's setpoint.

   In addition, an alarm sequence violation circuit is provided to ensure that the technician places the bistable output trip switch in trip prior to performing any testing on the analog section of the protection system. If this alarm actuates, it alerts the control room operator that the technician performing the surveillance is not following the proper procedural steps for testing. When this switch is in the normal position (not tripped), power is supplied through the bistable to both the train A and the train B logic cabinets.

7. Input Relays - The input relays are operated by the output of the bistable described in item 5 above. When energized (the bistable is not tripped), each input relay holds closed a contact in one of the logic matrices, providing circuit

continuity to reactor trip breaker undervoltage coils. When the protection bistable trips, its associated input relays de-energize, opening their corresponding contacts in the logic matrices.

In Figure 12.1-1, the red channel is shown from the sensor of some parameter to the inputs to the logic cabinets. For this discussion assume that the red channel is an analog process signal corresponding to pressurizer pressure. If this channel senses a pressure in excess of 2385 psig, its associated bistable trips, causing the bistable's output voltage to go to zero.

With the bistable output at zero, the red input relays de-energize in both the train A and train B logic cabinets. When the input relays de-energize, the contact labeled "1" opens in the logic matrix of train A, and the contact labeled "A" opens in the train B logic matrix. The logic coincidence for this particular trip function is two out of four (2/4). Therefore, two channels must de-energize to produce a reactor trip. Note that even with the 1 and A contacts open, power is still delivered from the 125-Vdc battery buses to the undervoltage (UV) coils for the reactor trip and reactor trip bypass breakers.

A reactor trip does not occur unless at least one of the other three channels also senses a high pressure condition, its associated bistable trips, and the associated input relays de-energize. With any two sets of logic matrix contacts open, power is interrupted to the undervoltage coils of the reactor trip breakers, causing them to open.

8. Logic Cabinets – The logic cabinets receive the signal inputs from the protection bistables (either on or off). The bistable output signals provide the protection system inputs for all reactor trips and ESF actuations. Energized input relays 1, 2, 3, and 4, (for train A) or A, B, C, and D, (for train B) hold their associated contacts closed, thereby maintaining continuity of power to the undervoltage coils of the reactor trip breakers. If an undervoltage coil de-energizes as the result of bistable trips, incorrect testing, or any other cause, one of the series-connected reactor trip breakers opens, allowing all shutdown and control rods to fall into the core.

9. Pushbuttons 1, 2, 3, and 4 (A, B, C, and D) – These buttons allow complete logic testing, which ensures the correct reactor trip breaker status when different combinations of channel trips are established. When an electronics technician depresses one of these pushbuttons, its associated test relay energizes, opening its associated test contact (shown beneath an input relay in Figure 12.1-1). When the test contact opens, the associated input relay de-energizes, causing its associated logic contact in the logic matrix to open. Using this process to satisfy the necessary trip coincidence (at least two input relays de-energized) ultimately interrupts power to a reactor trip breaker undervoltage coil. During this test, a reactor trip bypass breaker must be closed to prevent a reactor trip. The reactor trip breakers and their associated bypass breakers are described in section 12.1.3.3.

12.1.3.2 Solid-State Protection System

Applying solid-state techniques to the design of the reactor protection system has provided significant improvements over previous designs utilizing relays and contacts. Approximately 750 relays with 4000 contacts connected in various matrices are contained in a relay protection system for a Westinghouse-designed four-loop plant. This vast quantity of relays and contacts requires fourteen 30-in. wide by 30 in. deep cabinets, contrasted with six cabinets of the same size supplied with the solid-state system.

The addition of a semiautomatic fast pulse test circuit reduces the test time for the logic section of the protection system from four hours per train for the relay system to approximately one hour per train for the solid-state system. Fast pulse testing also eliminates the need to bypass the reactor trip breakers each time the logic section is tested. The duration of the logic test pulse is so short that the undervoltage driver card output is not interrupted. Therefore, the reactor trip breaker for the train undergoing this surveillance test is unaffected.

Figure 12.1-2 shows a simplified diagram of the solid-state reactor protection system. This system, like the analog reactor protection system, is comprised of two redundant, identical trains (A and B) that are physically and electrically independent. Inputs into this system are derived from various nuclear and nonnuclear sensors located both inside and outside of the containment building. Most of these signals are processed in the analog cabinets and result in bistable outputs (128 volts ac normal or zero volts when tripped) to the solid-state logic cabinets. Other protection signals are derived directly from the status of contacts at sensors or components (examples are oil pressure switches on the turbine, auxiliary contacts on circuit breakers, and limit switches on valves).

The physical arrangement of the input relay contacts within the logic portion of this system determines the coincidence logic (i.e., 2/3, 2/4, etc.). Additional inputs, which carry the train designation, enter the logic directly from control board switches and pushbuttons.

Information concerning the status of this system is transmitted to the control board status lamps and annunciators via a control board demultiplexing circuit and to the computer via a computer demultiplexing circuit. The purpose of these multiplexing systems is to transmit a large amount of status information over a small number of conductors, thereby simplifying and reducing field wiring requirements. About 200 status lamps and 100 annunciators are operated by the control board demultiplexer and about 200 signals are recorded by the plant computer by its demultiplexer.

Status information taken from the solid-state logic is transmitted to the demultiplexers through isolation devices in the trains (light transmission is used to achieve this isolation). The purpose of the isolation is to separate the monitoring circuit (which is considered to be a nonprotective function) from the protection circuitry. By design there is no possibility of short circuits, open circuits, or high voltage connections on the multiplexing line affecting operation of the protection circuits. The multiplexed outputs of the two trains are designed so that a status lamp or annunciator is actuated by either train A or train B. Normally both trains

actuate the devices simultaneously. A flashing lamp or annunciator indicates status disagreement between train A and train B.

The solid-state logic circuitry can be tested with the plant either shutdown or at power. Each train contains an identical semiautomatic test panel with the necessary controls for testing. During the logic matrix surveillance, all reactor trips and engineered safety features actuations for the train under test are inhibited (prevented from actuating). In addition, all information transmitted to the control board status lamps and annunciators, and to the plant computer from that same train, is inhibited. To perform this surveillance , the operator needs only to select the process to be tested using a rotary selector switch, press a “start test” pushbutton, and wait for either a green “good” lamp or a red “bad” lamp to illuminate. During the test sequence all possible combinations of nontrip and trip conditions for that process logic are checked.

The semiautomatic testing of the solid-state logic includes checking the continuity of power to the undervoltage coils of the reactor trip breakers and to the master relay coils, but excludes testing the input relays and contacts. The input relays and contacts are checked during testing of the analog portion of the protection system by tripping bistables while monitoring the control board status lamps for the specific tprotective functions. Since the lamps are operated through the multiplexing system, they cannot light unless appropriate input relays are affected.

12.1.3.3 Reactor Trip Breakers

Two series-connected reactor trip breakers, Figure 12.1-2, deliver power from the rod control motor-generator sets to the rod control power cabinets. A loss of power to these cabinets causes all rods to drop into the core.

Undervoltage coils keep the reactor trip breakers closed. In the untripped state, the reactor protection system logic matrices provide current flow paths to these coils. If a reactor trip coincidence is satisfied, contacts within the logic matrices open, breaking the continuity of these circuits, and the undervoltage coils de-energize. Removing power to these coils opens the reactor trip breakers.

Installed in parallel with each reactor trip breaker is a reactor trip bypass breaker. This presence of this breaker allows on-line testing of the associated reactor trip breaker without interrupting power to the rod drive mechanisms. The train A logic section supplies power to the undervoltage coils for the train A reactor trip breaker and for the train B bypass breaker. Similarly, the train B logic section supplies power to the undervoltage coils for the train B reactor trip breaker and for the train A bypass breaker. Whenever a reactor trip breaker is bypassed, the protection train associated with that breaker is considered to be inoperable.

The bypass breakers are interlocked so that if an attempt is made to close a bypass breaker with one reactor trip bypass breaker already closed, both bypass breakers trip open. This interlock prevents bypassing both protection trains simultaneously.

12.1.3.4 Output Cabinets

Engineered safety feature functions are generated from the protection system output cabinets (one for each protection train). Each output cabinet contains approximately 20 master relays and 40 slave relays. The logic section initiates an engineered safety features actuation by energizing master relay(s). Each master relay, in turn, operates contacts which energize up to four slave relays (see Figure 12.1-3). The slave relays close contacts in pump starting circuits, close contacts to open or close valves, or actuate solenoids for air-operated equipment.

Test cabinets for both the slave and master relays allow periodic testing. Testing of this circuitry consists of introducing a low voltage electrical signal to each coil. This low voltage is not strong enough to actuate the relay, but is sufficient to demonstrate continuity through the coil.

Integrated full-scale operability testing requires the actuation of the engineered safety features equipment (final device testing). Testing of this nature can only be accomplished during plant shutdown and requires extensive preparation and system realignments. Generally, one entire train (either train A or train B) is alternately tested every 18 months.

12.1.4 System Interrelationships

12.1.4.1 Protection System Testing

While only portions of this system are tested at any given time, the testing sequence provides an overlap to assure complete system operability. Testing the analog portion of the protection system at power is accomplished without initiating a protective action unless a trip condition actually exists. A trip does not occur because of the two-out-of-three or the two-out-of-four coincidence logic usually required for a reactor trip. Exceptions are the source and intermediate range high flux trip functions, which have one-out-of-two logic schemes. Therefore, placing one of these channels in test would generate a reactor trip. To prevent this action, these instruments have local bypass switches. However, placing one channel in bypass reduces the remaining function coincidence to one out of one.

Technicians verify the proper operation of process sensors by performing what is known as a channel check, which involves comparing redundant channels monitoring the same process variable to each other. Calibration of the sensors is normally accomplished during plant shutdown. The voltage and current of a channel from the sensor to the bistable is variable in magnitude and is referred to as the analog signal. From the bistable to the input relays, only ON-OFF signals are found. This portion of the channel is referred to as digital. Analog testing is performed at the analog instrumentation rack by individually introducing test signals into the instrumentation channels and observing the bistable outputs.

Each power range channel of the nuclear instrumentation system is tested by superimposing a test signal on the actual detector signal at the time of testing. The output of the bistable is not placed in a tripped condition prior to testing. Also, since

the coincidence logic for power range trip functions is two out of four, bypassing these functions is not required.

The logic trains of the reactor protection system are designed to be capable of complete testing at power, except for those trips listed below. Annunciation is provided in the control room to indicate when a train is in test, a reactor trip function is bypassed, or a reactor trip bypass breaker is racked in and closed.

The reactor coolant pump breakers cannot be tripped at power without causing a reactor trip. However, the reactor coolant pump breaker open trip logic and continuity through the shunt trip coil can be tested at power. The manual reactor trip switches cannot be tested at power without causing a reactor trip, since operation of either manual trip switch actuates both trains of the protection system. Initiating a safety injection actuation or a turbine trip cannot be performed at power without upsetting normal plant operations. However, the logic for these trips is testable at power.

All trip function channels, logic trains, and trip breakers of the RPS are normally required to be in service. However, to permit on-line testing of the various system portions or to permit continued operation in the event of a failure, the Technical Specifications allow continued plant operation with limited RPS inoperabilities. The Technical Specifications also define the required restrictions on operation in the event that the full system operability is not met.

The RPS is designed so that response-time tests can only be performed during shutdown. However, the safety analysis includes conservative numbers for trip channel response times. The measured channel response times are compared with those used in the safety evaluations. On the basis of startup tests conducted at several plants, the actual response times measured are less than the times used in the safety analyses.

12.1.4.2 Testing Input Relays

Testing the logic trains of the reactor protection system includes a check of the input relays and a logic matrix check. During a process instrumentation system test, the technician trips each bistable. Each tripped bistable de-energizes one input relay in logic train A and one input relay in train B. A contact from each relay is connected to a universal logic printed circuit card. This printed circuit card performs both trip and monitoring functions. The contact that creates the channel trip signal also actuates a status lamp and an annunciator on the control board. Operation of the input relay from either train lights the status lamp and the annunciator.

Each train contains a multiplexing test switch. At the start of a process or nuclear instrumentation system test, this switch (in either train) is placed in the A+B position. The A+B position alternately transmits information from the two trains to the control board. A steady status lamp and annunciator indicates that the input relays in both trains have been de-energized. A flashing lamp means that the input relays in the two trains have not both de-energized. Contact inputs to the protection system logic, such as reactor coolant pump bus under-frequency relays, operate input

relays which are tested by operating the remote contacts and using the same type of indications as those provided for bistable input relays.

Actuation of the input relays provides the overlap between testing the logic portion of the protection system and testing those systems supplying the inputs to the logic section. Inputs to the logic section are checked one channel at a time, leaving the other channels in service. For example, a function that trips the reactor when two out of four channels trip effectively becomes a one-out-of-three trip when the channel in test is placed in the trip mode. Both trains of the logic section remain in service during this portion of the test.

12.1.4.3 Testing Logic Matrices

Logic matrices are checked one train at a time. Input relays are not operated during this portion of the test. Reactor trips from the train under test are inhibited by the input error inhibit switch on the semiautomatic test panel in the train. At the completion of the logic matrix tests, one bistable in each channel of process instrumentation or nuclear instrumentation is tripped to check closure of the input error inhibit switch.

The logic test scheme uses short duration pulse techniques to check the coincidence logic. All possible trip and nontrip combinations are checked. Pulses from the tester are applied to the inputs of the universal logic card at the same terminals that connect the input relay contacts. Thus, there is an overlap between the input relay check and the logic matrix check. Pulses are fed back from the reactor trip breaker undervoltage coil to the tester. These pulses are of such short duration that the reactor trip breaker undervoltage coil armature cannot respond mechanically.

12.1.4.4 Testing Reactor Trip Breakers

Normally, reactor trip breakers A and B are in service, and their associated reactor trip bypass breakers A and B are open and racked out (out of service). The following procedure briefly describes the method used for testing the reactor trip breakers:

1. With reactor trip bypass breaker A racked out, manually close and trip this breaker to verify its operability.
2. Rack in and close reactor trip bypass breaker A. Trip reactor trip breaker A using the protection system logic matrix.
3. Re-close reactor trip breaker A.
4. Trip (open) and rack out reactor trip bypass breaker A.
5. Repeat the above steps to test reactor trip breaker B.

Auxiliary contacts of the reactor trip bypass breakers supply a protective function designed to prevent both bypass breakers from being closed simultaneously. If either train is placed in test while the reactor trip bypass breaker of the other train is closed, both reactor trip breakers and both reactor trip bypass breakers automatically trip.

12.1.4.5 Testing Bypasses

Where operating requirements necessitate automatic or manual bypass of a protective function, the system is designed so that any actuated bypass is automatically removed whenever permissive conditions are not met. Devices used to achieve automatic removal of the bypass of a protective function are considered part of the protection system and are tested much as other RPS components are tested. Indication is provided in the control room if some part of the system has been administratively bypassed or taken out of service.

12.1.5 PRA Insights

The purpose of the reactor protection system is to initiate reactor trips to prevent the plant from exceeding a safety limit and to actuate engineered safety features to mitigate the consequences of an accident. A failure of the reactor protection system would allow core heat production to continue and prevent the initiation of safety-related heat removal systems. Therefore, the failure of the RPS could lead to significant core damage.

The failure of the reactor protection system is not a significant contributor to sequences which lead to core damage (6.3% at Surry, 1.3% at Sequoyah). However, the failure of the reactor protection system to perform its function has a major impact on importance measures. The risk achievement factor is 1300 for Surry and 450 for Sequoyah.

12.1.6 Summary

Due to its importance to safety, the RPS is designed, constructed, and tested to the highest standards. These include requirements for the ability to withstand single failures and still provide full protection, for the independence of separate trains, and for testability to insure continued reliability.

The RPS contains process sensors (multiple sensors for each parameter) which produce variable outputs provided to comparators (bistables). The variable signal from a sensor is compared to a preset bistable trip setpoint. If the process variable exceeds the setpoint value, the bistable changes state and de-energizes (its output voltage goes to zero). The bistables's output is sensed by both the train A and train B logic cabinets.

The logic cabinets continuously monitor the status of the bistables and produce a protective action (reactor trip or ESF actuation) when the coincidence of tripped bistables indicates the need for it. Either logic train, by itself, is sufficient to fully initiate necessary protective actions independent of the other logic train.

Testing the RPS at power is necessary to ensure the continued reliability and integrity of the RPS. Testing is performed by overlapping individual tests of system portions to ensure that nothing is missed. Sensor calibration and final device testing is normally performed when the plant is shutdown.

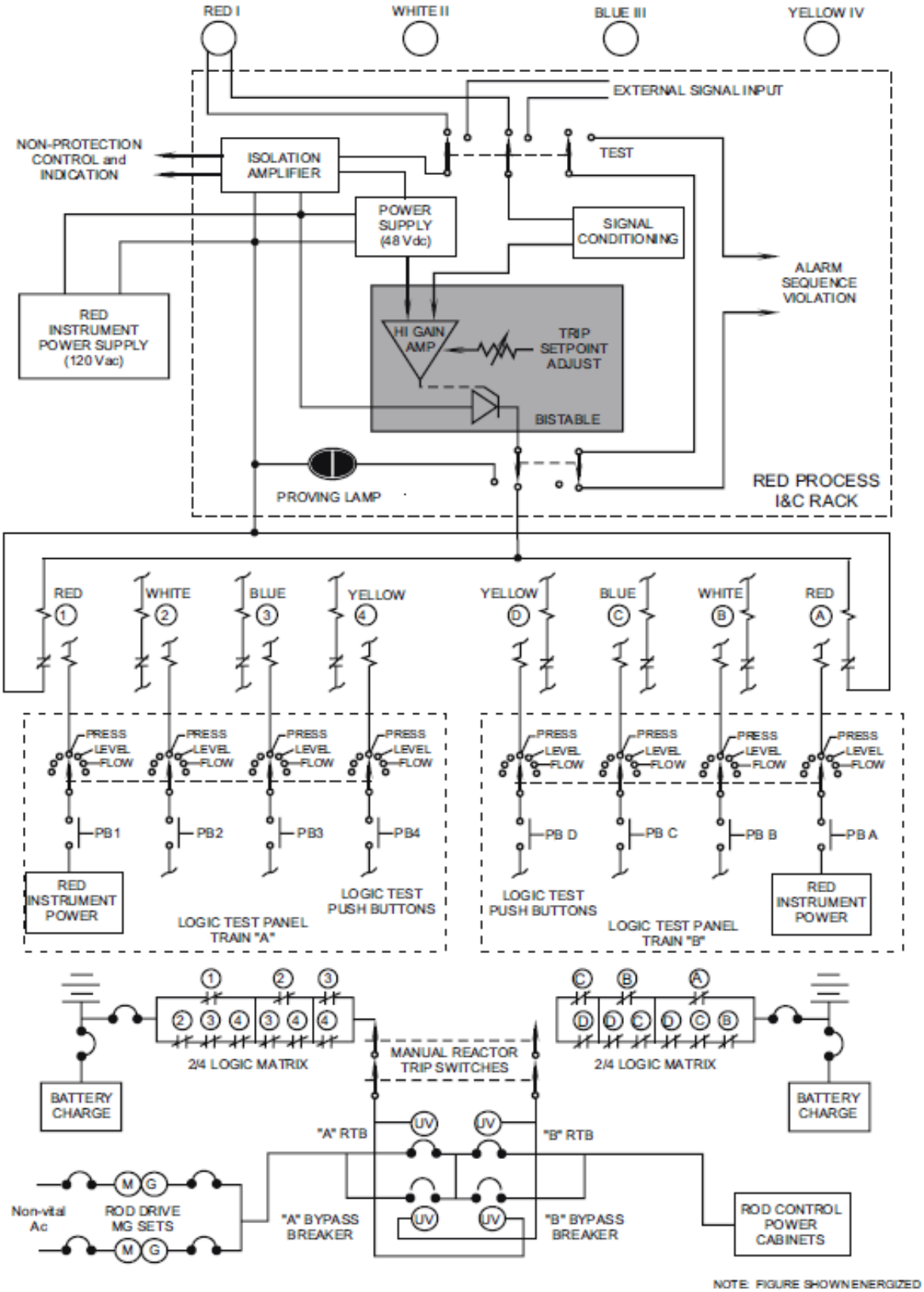

Figure 12.1-1 Relay Protection System

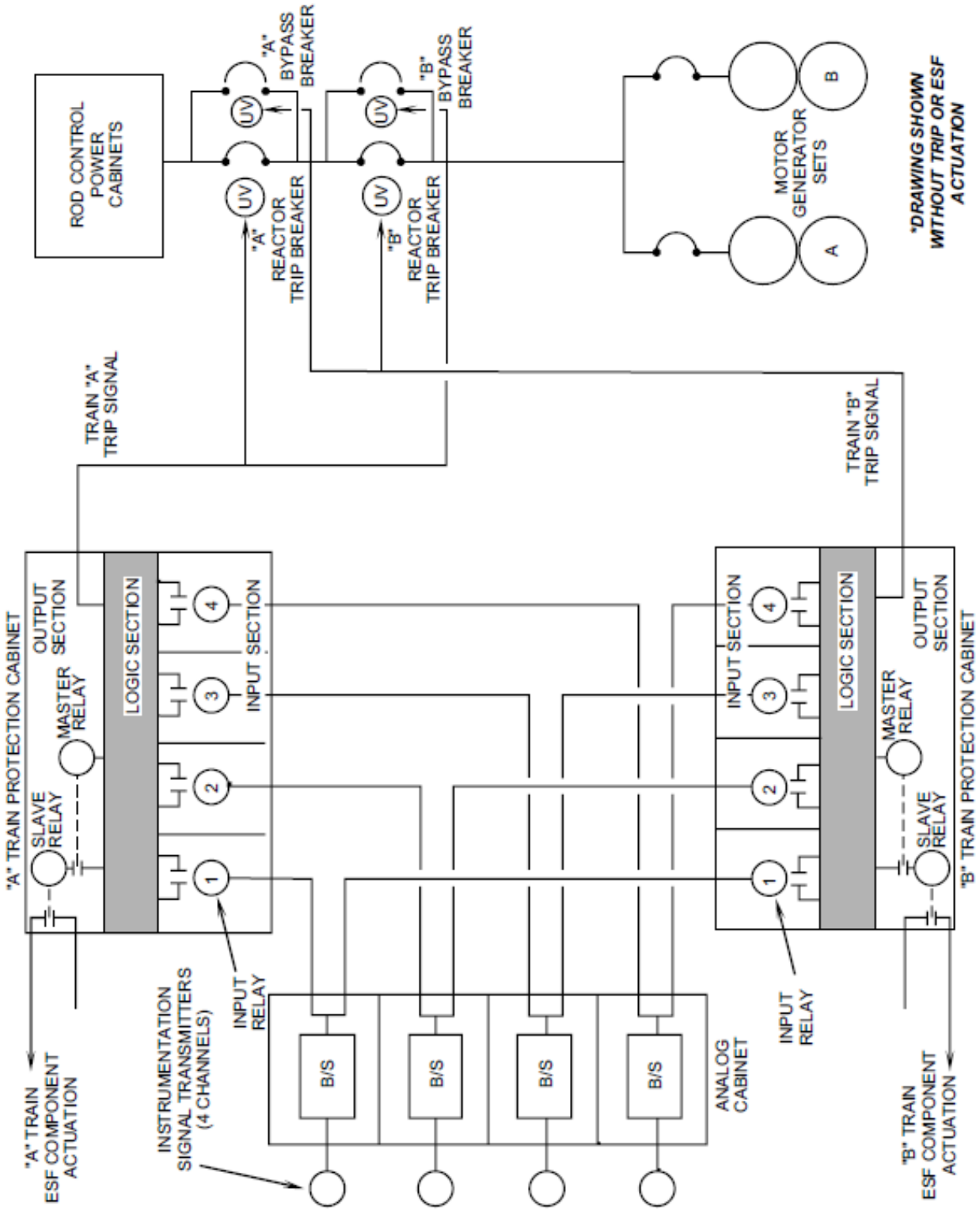

Figure 12.1-2 Solid State Protection System

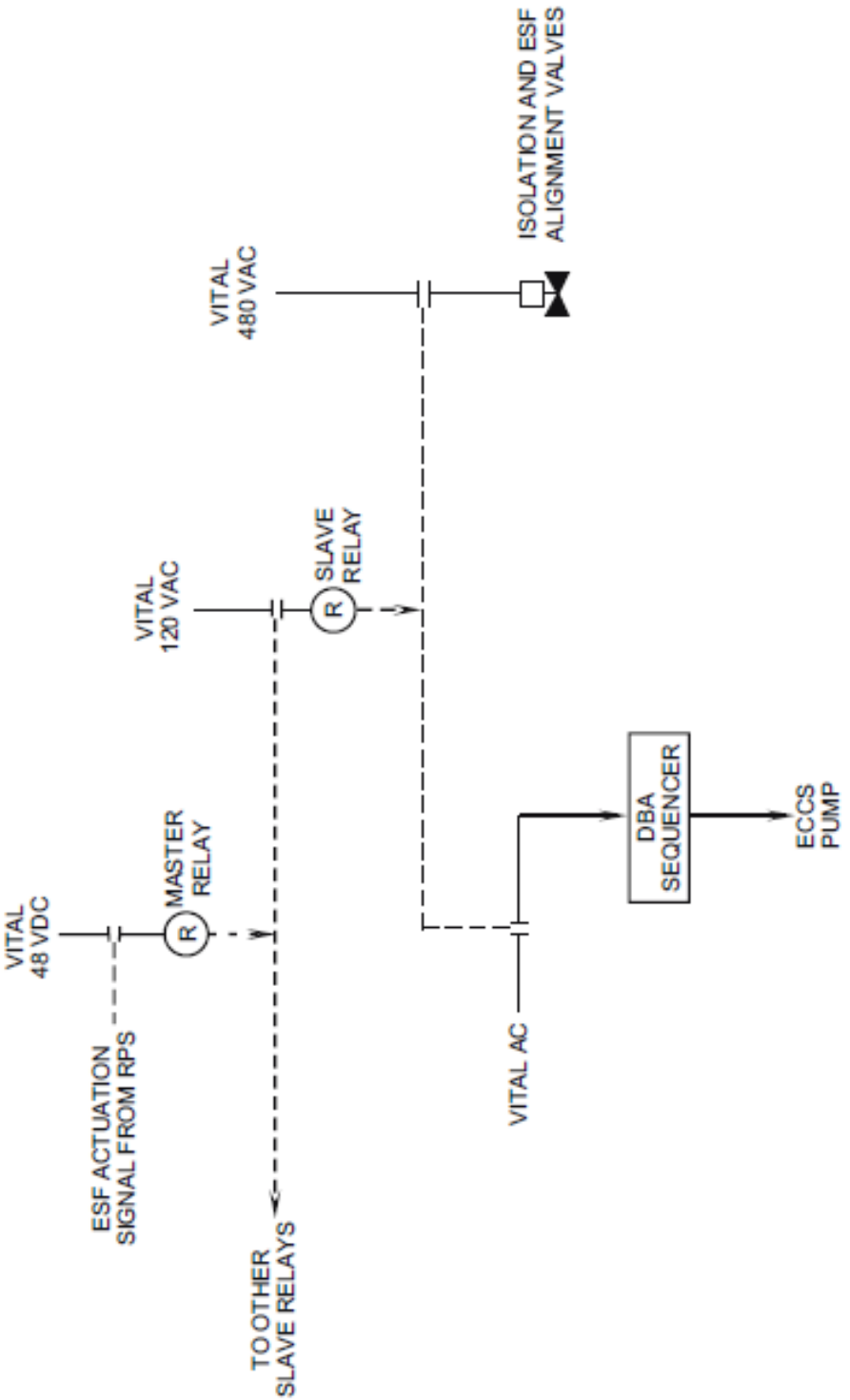

Figure 12.1-3 ESF Actuation Output Relay Operation