TABLE OF CONTENTS

LIST OF FIGURES

This page intentionally blank

4.7.0 Anticipated Transient Without Scram (ATWS)

Learning Objectives:

1. Define the term "anticipated transient without scram" (ATWS).
2. Describe the limiting (most severe) ATWS case for a pressurized water reactor (PWR).
3. List three parameters or components that affect a plant's sensitivity to an ATWS event.
4. Describe the modification made to Westinghouse reactor trip breakers after the Salem ATWS.
5. State the functions of the ATWS mitigation system.
6. List three event tree considerations (headings) used in estimating the conditional core damage probability of ATWS sequences.

This page intentionally blank

4.7.1 Introduction

The definition for the term "anticipated transient without scram" can be found in 10CFR50.62, commonly known as the "ATWS rule." An ATWS is defined as an anticipated operational occurrence as defined in 10CFR50, Appendix A, followed by the failure of the reactor trip portion of the protection system specified in General Design Criterion 20 of Appendix A.

The term "transient" applies to any significant deviation from normal values of any of the key operating parameters. A transient may occur as a result of equipment failure or malfunction, or as the result of an operator error. Anticipated operational occurrences are further classified as Condition I and II events in ANSI 18.2. These events are expected to occur one or more times during the life of the plant.

Many transients are handled by various reactor control systems, which return the reactor to its normal operating condition. However, the more severe transients require that the reactor be shut down by the reactor protection system (RPS). As stated in the technical specification basis for reactor trip system instrumentation, the reactor trip avoids damage to the reactor fuel and cladding or to the reactor coolant system pressure boundary.

4.7.2 Reactor Protection System Design

The Westinghouse reactor protection system is shown in Figure 4.7-1. As shown, power to the control rod drive mechanisms (CRDMs) is supplied by motor generator sets through two series reactor trip circuit breakers. The opening of either reactor trip breaker de-energizes all CRDMs, and the reactor trips. This trip scheme is an example of one-out-of-two logic; it requires the actuation of only one protection train and the opening of only one reactor trip circuit breaker, at a minimum, to trip the reactor.

While this logic provides redundant means of generating a reactor trip, the testing of a reactor trip circuit breaker would result in a reactor trip without some compensating measure. Since testing is required, the RPS design includes bypass breakers that are manually installed during testing. For example, if a test of the A reactor trip breaker is required, a bypass breaker is racked in to provide a circuit path parallel to that of the A trip breaker to ensure continuity of power when the trip breaker is opened. The A bypass breaker is opened by the B protection train; therefore, during testing the reactor protection system is reduced to one-out-of-one logic.

The protection system consists of a number of analog channels. The analog section receives input signals from transmitters that sense process parameters. Each process signal is compared to a setpoint in a bistable. If the monitored parameter's input signal is equal to or exceeds the setpoint, a trip signal is generated by the bistable. The bistable trip signal is sent to redundant logic cabinets, where the reactor trip actuation signals are generated.

Each reactor trip function has a coincidence network; only one such network is shown in each protection cabinet of Figure 4.7-1. This coincidence is two-out-of-four logic. Assume that the instrument transmitters are supplying pressurizer pressure signals. If instrument transmitter 1 senses a high pressure condition (greater than the high pressure trip setpoint), its associated bistable trips. Both logic cabinets receive this signal and open the contacts associated with this channel. If no other contacts are open in this logic matrix, the undervoltage coils remain energized, and no trip occurs. If another transmitter also indicates a high pressure condition, its associated bistable trips, and now the necessary two-out-of-four logic is satisfied. When this occurs, vital power is interrupted to the undervoltage coils, allowing the reactor trip breakers to open.

4.7.3 ATWS Historical Background

The ATWS event became a possible source of concern for nuclear power plants in 1968 during discussions between the Advisory Committee on Reactor Safety (ACRS), the regulatory staff, and reactor instrument designers. There were various concerns, one of which was the possibility of interactions between control and protection functions in the instrumentation systems. After considerable discussion and some design changes, it was determined that separation of control and protection functions was being achieved to a reasonable degree, either by physical separation or electrical isolation.

The focus of interest with regard to instrumentation systems then shifted to the ability of the shutdown systems to function with the needed reliability considering common-mode failures. Common-mode failures are failures due to design deficiencies or maintenance errors that could render inoperable redundant components or portions of a safety system. At the time, it was difficult to determine whether a common-mode failure was adequately accounted for partially because the techniques to analyze such failures were not fully developed.

In 1969, the efforts to evaluate the safety concerns of the ATWS events were divided into two areas. One area was concerned with attempting to evaluate the likelihood of common-mode failures or any other failure of the reactor protection system. The second area was to analyze the consequences of various postulated ATWS events.

The ATWS event was analyzed in combination with different initiating conditions. The results showed that the worst-case ATWS initiating event for a pressurized water reactor is a loss of main feedwater.

A loss of main feedwater normally results in a reactor trip to prevent a loss of heat sink. The signal input to the reactor protection system to indicate that a loss of heat sink has occurred is a low-low level in one or more of the steam generators. However, the ATWS analysis assumes that a common-mode failure occurs which prevents the proper operation of the reactor protection system, and the reactor does not automatically trip.

With the loss of heat removal by the steam generators and the lack of a reactor trip, energy from the reactor causes a rapid increase in the reactor coolant temperature. The resultant coolant expansion causes an insurge into the pressurizer, which compresses the pressurizer steam volume. The compression of the pressurizer steam space causes the pressure in the reactor coolant system to rapidly increase. Since systems such as the rod control and pressurizer pressure control systems are not safety-grade, no credit is taken for their action. Therefore, as the temperature continues to increase, the pressure in the reactor coolant system also continues to increase.

As the primary temperature increases, the steam generator pressure increases. The increased secondary pressure causes the steam line code safety valves to open. Even though the auxiliary feedwater system is discharging to the steam generators, the feed rate is insufficient to match the rate of mass loss through the safety valves. The result of the steam generators drying out is that the reactor coolant system temperature increases at a faster rate.

For a reactor with a negative moderator temperature coefficient (MTC), the increasing reactor coolant system temperature adds negative reactivity, which decreases reactor power. Unfortunately, the decrease in reactor power and resultant tempering of the coolant temperature increase are not enough to prevent the pressurizer from filling. When the pressurizer is completely filled, or becomes water solid, an increasing reactor coolant temperature results in a very high reactor coolant system pressure. For all PWR analyses, pressures in excess of 3000 psia are reached. Since this pressure is in excess of the design pressure (2500 psia) of the reactor coolant system, there is a concern about possible system damage and degradation of the emergency core cooling system interfaces.

The severity of an ATWS (peak pressure reached) initiated by a loss of feedwater is affected by the following parameters:

1. The value of the moderator temperature coefficient,
2. The size of the pressurizer,
3. The size of the pressurizer safety valves,
4. The secondary inventory, and
5. The main turbine status (operating or tripped) during the transient.

The value of the moderator temperature coefficient determines whether and how much negative reactivity is added (and the resultant reactor power decrease) as the reactor coolant temperature increases. Therefore, the worst case for the transient is at the beginning of core life (especially for high burnup cores), when the moderator temperature coefficient can be positive, or negative with a small magnitude.

The pressurizer volume is important from the standpoint of the time required to reach the solid-water condition. The size of the code safety valves determines the amount of coolant outflow when the system becomes solid. If the capacity of the code safety valves is small, then the ultimate pressure reached in the reactor coolant system will be higher.

The amount of mass in the secondary side of the steam generators determines the dry-out time of the steam generators. As previously discussed, after the steam generators dry out, the heat sink for the reactor coolant system is lost, and reactor coolant system pressure rapidly increases.

The severity of the accident is also affected by whether the main turbine is operating. It would appear that the loss of feedwater transient would be less severe if the main turbine remains in service, so that additional heat is removed from the reactor coolant system. However, this heat removal path results in a loss of steam generator inventory and decreases the time required to dry out the steam generators. A shorter dry-out time increases the pressure reached in the reactor coolant system during the loss of feedwater transient.

Intuitively, it would appear that the possibility of reaching these high reactor coolant system pressures during a loss of main feedwater is extremely small. After all, the loss of main feedwater transient and some common-mode reactor protection system failure must occur simultaneously. Electric Power Research Institute report NP-2230 (1982) calculated a frequency of 0.15/yr for total loss of main feedwater events, based on from 36 operating PWRs. The error in this data is not known, because all loss of feedwater events are not reported. The failure of the reactor trip circuit breakers, the interrupting device of the reactor protection system, has occurred many times at operating plants. Data from NUREG-1000, "Generic Implications of ATWS Events at the Salem Nuclear Power Plant" (1983), show that out of 16,000 breaker demands at pressurized water reactor plants, a total of 53 failures had occurred.

4.7.4 Operational Occurrences

4.7.4.1 Salem ATWS

Simultaneous failures of the reactor trip breakers occurred at the Salem nuclear plant on February 22, 1983. The unit was operating at 20% power with one main feed pump in service. The second main feed pump was at minimum speed in preparation for continued power escalation. The operators were in the process of transferring loads from offsite power to the unit generator. During the transfer, a limit switch failed, causing the loss of one of the nonvital buses. Immediate equipment losses included one reactor coolant pump, control power to the operating main feedwater pump, control room lighting, and a 125-Vac miscellaneous distribution panel.

The loss of the distribution panel caused a loss of nonvital indications in the control room, which included the main feedwater pump indications and the steam generator panel (feed flows and steam flows). However, steam generator water level indications were still available.

The loss of main feedwater resulted in decreasing steam generator levels, and the low-low level trip setpoint was reached. This resulted in a trip signal being generated by the reactor protection system. However, the two series reactor trip circuit breakers failed to open. After evaluating the deteriorating plant conditions, the operator manually tripped the plant. The operator took action 3.5 seconds after the trip signal generated by the reactor protection system, thereby masking the failure of the trip breakers to open automatically. Since the reactor tripped when the operator actuated the manual trip switch, plant personnel did not suspect a problem with the reactor trip system, and, therefore, the ATWS went unnoticed until February 25, 1983.

On February 25, 1983, Salem was operating at 12% reactor power with the feedwater system in manual control. Difficulty in controlling steam generator levels was experienced, and the level in one of the four steam generators dropped to the low-low level reactor trip setpoint. Again, the reactor trip circuit breakers failed to open. The operator, after observing the first-out annunciator, announced on the plant paging system that a plant trip had occurred.

Another operator in the control room noticed that the reactor had not tripped, as indicated by the unlit rod bottom lights. In addition, the turbine had not tripped as expected. The shift supervisor monitored the steam generator levels at this time and noticed that they were at the low-low level trip setpoint (18%). He then directed the reactor operator to manually trip the plant. The operator tripped the plant 23 seconds after the original trip signal was generated.

The shift supervisor was concerned that a failure of the first-out annunciator system or of the reactor protection system had occurred. The instrumentation department was called to perform tests to determine the apparent problem with the indications described above. After the steam generator level bistables and the protection system were verified to be operating properly, tests were performed on the reactor trip breakers. When the trip breakers failed to open when demanded by the protection system, it was determined that an ATWS had occurred.

4.7.4.2 Breaker Malfunction

In both events at Salem, the reactor trip circuit breakers failed to function as designed. Figure 4.7-2 shows the reactor trip circuit breaker design at the time of the events. During normal operations, the circuit breakers are closed, supplying power to the control rod drive mechanisms. Each circuit breaker's undervoltage coil is energized and holds the main trip shaft in position as shown. The power keeping the undervoltage coil energized is controlled by the RPS.

When a trip signal is generated through the appropriate logic (two out of three or two out of four), the RPS de-energizes the undervoltage coil, which releases the main trip shaft. The spring shown directly above the undervoltage coil pulls on the arm it is attached to, causing the main trip shaft to rotate in the counterclockwise direction. When this shaft rotates, it allows the trip spring to pull the top portion of the trip bar to the left, which opens the reactor trip breaker.

Opening the reactor trip circuit breakers removes power from the power cabinets, de-energizing the stationary and movable grippers, and allowing the rods to fall into the core. The undervoltage coil provides a fail-safe feature of the reactor protection system: if a loss of power to the reactor protection system should occur, the undervoltage coils would de-energize, and the reactor trip breakers would open as described above. In the Salem ATWS, the undervoltage coils operated properly, but because of mechanical interference, the reactor trip circuit breakers failed to open as designed.

In addition to the undervoltage coil, each reactor trip breaker has an associated shunt trip coil. The shunt trip coil is normally de-energized when the breaker is closed. To open the breaker with the shunt trip coil, it must be energized. Energizing the coil pulls the shunt trip lever down. As this lever moves down, it comes in contact with the main trip shaft, which is forced to rotate in the counterclockwise direction. As explained above, this starts the chain of events which causes a reactor trip.

In the original Westinghouse design, the remote reactor trip switch opens the reactor trip circuit breaker by energizing the shunt trip coil, while simultaneously de-energizing the undervoltage coil. This manual trip feature allowed the operator to trip the reactor from the control room during both ATWS events at Salem.

The incident that occurred at Salem resulted in increased surveillances of reactor trip breakers to ensure operability. During surveillance testing at McGuire in July of 1987, one reactor trip breaker failed to open when tripped from the control room. It was found to have a defective weld on the trip shaft, which resulted in the mechanical binding of the trip shaft. This prevented the breaker from opening.

Upon further investigation, the other trip breakers at the McGuire station were found to have defective welds on their trip shafts. NRC Bulletin 88-01 was issued on February 5, 1988, to alert utilities using Westinghouse DS model trip breakers that a potential problem existed with this design.

4.7.5 Plant Modifications

4.7.5.1 Reactor Trip Breakers

As shown in Figure 4.7-2, the original Westinghouse design provided only one means by which the RPS would automatically open the reactor trip breakers: the de-energizing of the undervoltage coils. In the aftermath of the Salem events, trip breaker operation was modified to provide redundant means of automatically opening the breakers. With the modification, shown in Figure 4.7-3, the reactor protection system both energizes the shunt trip coil and de-energizes the undervoltage coil for each breaker when trip logic is satisfied.

4.7.5.2 ATWS Rule Requirements

10CFR50.62, published in 1984 and commonly referred to as “the ATWS rule,” imposed new equipment requirements for all PWRs, as discussed in the following paragraphs.

4.7.5.2.1 Diverse Trip System

Combustion Engineering (CE) and Babcock and Wilcox (B&W) designed pressurized water reactors are required to have a second, diverse trip system. The system is required to be independent of the RPS from the sensor outputs to the CRDM power supplies. The diverse trip system has been imposed as a defense-in-depth measure for CE and B&W plants because of the relatively high percentage of fuel cycle time those plants are expected to operate with positive or slightly negative MTCs (in accordance with analyses performed by the reactor plant designers at the time of the ATWS rule). If an ATWS occurs when the MTC is positive or insufficiently negative to limit the reactor power and the associated increase in reactor coolant pressure, ATWS mitigation systems are likely to be ineffective. Westinghouse designed plants have been excluded from this requirement because of their larger pressurizer safety valves and relatively smaller expected percentage of fuel cycle time with positive or only slightly negative MTCs. (Refer to the discussion in section 4.7.3 of this chapter regarding the impacts of MTC and pressurizer relief valve capacity on the severity of an ATWS.)

A typical B&W diverse trip system interrupts power to the CRDMs when a very high reactor coolant system pressure setpoint has been reached. The very high pressure setpoint reflects the coolant expansion and high pressure expected during an ATWS event.

4.7.5.2.2 ATWS Mitigation System

Paragraph (c) of 10CFR50.62 requires each pressurized water reactor to have "equipment from sensor 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."

In response to the ATWS rule, an ATWS mitigation system has been installed in each PWR to provide a backup to the reactor trip system and the engineered safety features actuation system for initiating a turbine trip and actuating the auxiliary feedwater system in the event of an ATWS. The system is typically non-safety-related, powered by non-Class 1E source, and microprocessor based. Various signals, such as high reactor coolant system pressure and low steam generator level, can be used as indications of an ATWS event. Two examples of ATWS mitigation systems are described below.

The Trojan ATWS mitigation system actuating circuitry (AMSAC), shown in Figure 4.7-4, starts the turbine-driven and diesel-driven auxiliary feedwater pumps and trips the main turbine if the narrow-range steam generator levels drop below the low-low level setpoint (11.5%) for at least 25 seconds in three of the four steam generators. This circuit is only functional when load is greater than 40% and for 6 minutes after load is reduced to less than 40%.

The Indian Point Unit 3 AMSAC (see Figure 4.7-5) performs the same functions as the system described above. However, instead of steam generator narrow-range levels, main feedwater flows are supplied as inputs. If main feedwater flows drop below 21% in three out of four channels for a preset length of time (depending on power level), and power is greater than 40% as indicated by turbine impulse pressure, the turbine is tripped, the auxiliary feedwater system is actuated, and the steam generator blowdown and sample lines are isolated. The signal is maintained for 40 seconds or for as long as the activation criteria are met. The 40-second timer maintains the AMSAC initiation signal to ensure that the necessary actions occur under changing conditions of power and feedwater flow.

Because the design of the ATWS mitigation system utilizes application software and intelligent automation controllers, problems have been encountered with the system that are unlike others traditionally experienced at nuclear plants. For example, in December of 1992, the Indian Point Unit 3 AMSAC was found to be inoperable since July of 1992 because of a software problem resulting from significant deficiencies in maintenance, testing, and quality assurance of the system. The configuration for the system is maintained on a hard drive, and it automatically loads into memory upon boot-up. The hard drive failed to reboot during a surveillance test in May of 1992. The utility reinstalled the repaired hard drive after it was returned from the vendor. The configuration files had to be rebuilt from an uncontrolled copy of the files kept by a vendor technician, because the utility had not maintained a controlled copy. During performance of post-maintenance testing on the system, the automatic reboot function was tested. However, the AMSAC developed a faulty trip signal and failed the test. Subsequent to software manipulations made by the vendor to address the faulty signal, only the reboot function was tested. During the next scheduled surveillance test in December of 1992, it was discovered that the AMSAC auxiliary feedwater initiation was inoperable due to inadvertent misplacement of the the 40-second timer in the system software during the software manipulations that had been conducted during the previous July. The system software was corrected, and the AMSAC was returned to an operable status in January of 1993.

4.7.6 PRA Insights

4.7.6.1 Historical

The NRC staff evaluation of ATWS in NUREG-460, “Anticipated Transients Without Scram for Light Water Reactors” (1980), was one of the first applications of PRA techniques to an unresolved safety issue. The evaluation highlighted the relative frequency of severe ATWS events associated with various reactor types and estimated the expected reduction in frequency for various postulated plant modifications. The study also proposed quantitative goals for resolving this issue. Other notable examples of PRA applications to the ATWS issue are the NRC sponsored survey and critique of reactor protection systems (SAI, 1982), and the ATWS Task Force report summarized in SECY-83-293.

The RPS survey reviewed 16 reliability studies, most of them published PRAs, to compare the predicted failure probability per unit demand, the anticipated transient frequency, and the primary influences on RPS unavailability. There was a surprising degree of agreement among the 16 studies. A second study quantified the relative improvement to be gained by implementing a set of recommendations proposed by a utility consortium in an ATWS petition to the NRC. A third study, a value-impact evaluation of the risk reduction of generic plant classes, provided the basis for the final rule on ATWS (SECY-83-293).

A recently prepared draft NRC Office of Nuclear Regulatory Research report assesses whether the ATWS rule and other relevant Commission recommendations issued with the ATWS rule have been effective in achieving the desired outcomes. The report concludes that the ATWS rule and associated recommendations have been effective in having the required plant modifications installed, in reducing core damage frequency associated with ATWS, and in limiting the costs to licensees. Specifically:

- Hardware modifications required by the ATWS rule have been implemented at all PWRs, typically between 1986 and 1990, including the diverse means of tripping the turbine and initiating auxiliary feedwater at all plants and the diverse scram system at CE and B&W plants. The report notes that changes in fuel design to achieve longer operating cycles will result in less negative MTCs for a larger fraction of the cycle time, during which ATWS mitigation functions may be rendered ineffective. Fuel cycle changes that significantly increase the ATWS risk due to longer exposure to such MTCs may require compensatory measures consistent with the ATWS rule for Westinghouse plants.

- SECY-83-293 set a goal of 1.0E-05/RY for the core damage frequency associated with an unmitigated ATWS (referred to as P(ATWS)). This goal has been exceeded for all plant types; the average Westinghouse plant value is 6.4E-07/RY. The reduction in P(ATWS) has been greatly affected by the large decrease in the frequency of automatic trips (the initiating events for ATWSs) since the ATWS rule was invoked. Also, better than expected improvements in RPS reliability have been achieved for all reactor plant types.

- RPS reliability is related to reactor trip breaker reliability. As evidenced by NRC generic communications and industry group activities, circuit breaker problems continue to occur. Industry programs to maintain RPS reliability continue to be useful in limiting risk from ATWSs.
- However, RPS reliability estimates are subject to large uncertainties. RPS reliability requirements are so high and ATWS events are so rare that many more years of operating experience are needed to generate sufficient system demands to reduce current estimates of the uncertainty. The current uncertainty associated with RPS reliability argues for the continued application of the requirements of the ATWS rule.
- Costs associated with implementing the ATWS rule have been less than expected ($166M actual vs. $354M expected), largely due to fewer than expected spurious trips caused by ATWS mitigation equipment.

NUREG-1560, “Individual Plant Examination Program: Perspectives on Reactor Safety and Plant Performance” (1997), concludes that ATWS is not an important contributor to the total core damage frequency for almost all Westinghouse plants. The core damage frequency attributable to ATWS events is small in absolute terms for almost all plants, and constitutes a significant contribution to total core damage frequency (greater than 10%) for just two plants. Each of these plants, Beaver Valley 1 and Indian Point 3, operates with some or all of its power-operated relief valve block valves closed, thereby reducing the relief capacity of the reactor coolant system during the early stages of an ATWS and thus increasing the potential peak pressure reached.

4.7.6.2 Plant Event

On June 3, 1991, a low flow reactor trip signal was generated during the calibration of a reactor coolant system flow instrument at Harris Unit 1 (LER 400/91-010). The B reactor trip breaker opened as required, but the A trip breaker failed to respond. The failure was due to a failed circuit board (a result of previous improper maintenance). The board failure prevented the occurrence of the automatic undervoltage and automatic shunt trips of the associated reactor trip breaker. A manual trip was still available.

Assuming that both reactor trip breakers had failed to open, the conditional probability of subsequent core damage was estimated at 6.6E-06 for this event. Figure 4.7-6(a) shows the relative significance of this event compared to other postulated events at Harris Unit 1.

The model used to estimate the conditional core damage probability is shown in Figure 4.7-6(b). Assuming that an ATWS occurs with no manual trip (the operator does not perform the actions as directed by the emergency procedures), four sequences have end states of core damage. The dominant sequence for core damage is sequence 2, which assumes an ATWS, no operator action to insert the control rods, that primary pressure is limited, that the auxiliary feedwater system operates, but that emergency boration is not initiated.

4.7.7 Summary

The ATWS event is an analyzed plant transient that requires the automatic shutdown of the plant, combined with the failure of the reactor protection system to respond as designed. The Code of Federal Regulations requires that each pressurized water reactor must have equipment, that is diverse from the reactor trip system, that will initiate the auxiliary feedwater system and trip the turbine under conditions indicative of an ATWS. Therefore, utilities have installed ATWS mitigation systems that perform those functions.

As a result of the Salem ATWS, Westinghouse units added the automatic energizing of the shunt trip coil by the RPS. This modification provides a redundant means of opening the reactor trip breakers and potentially reduces the probability that a common-mode failure would prevent their opening.

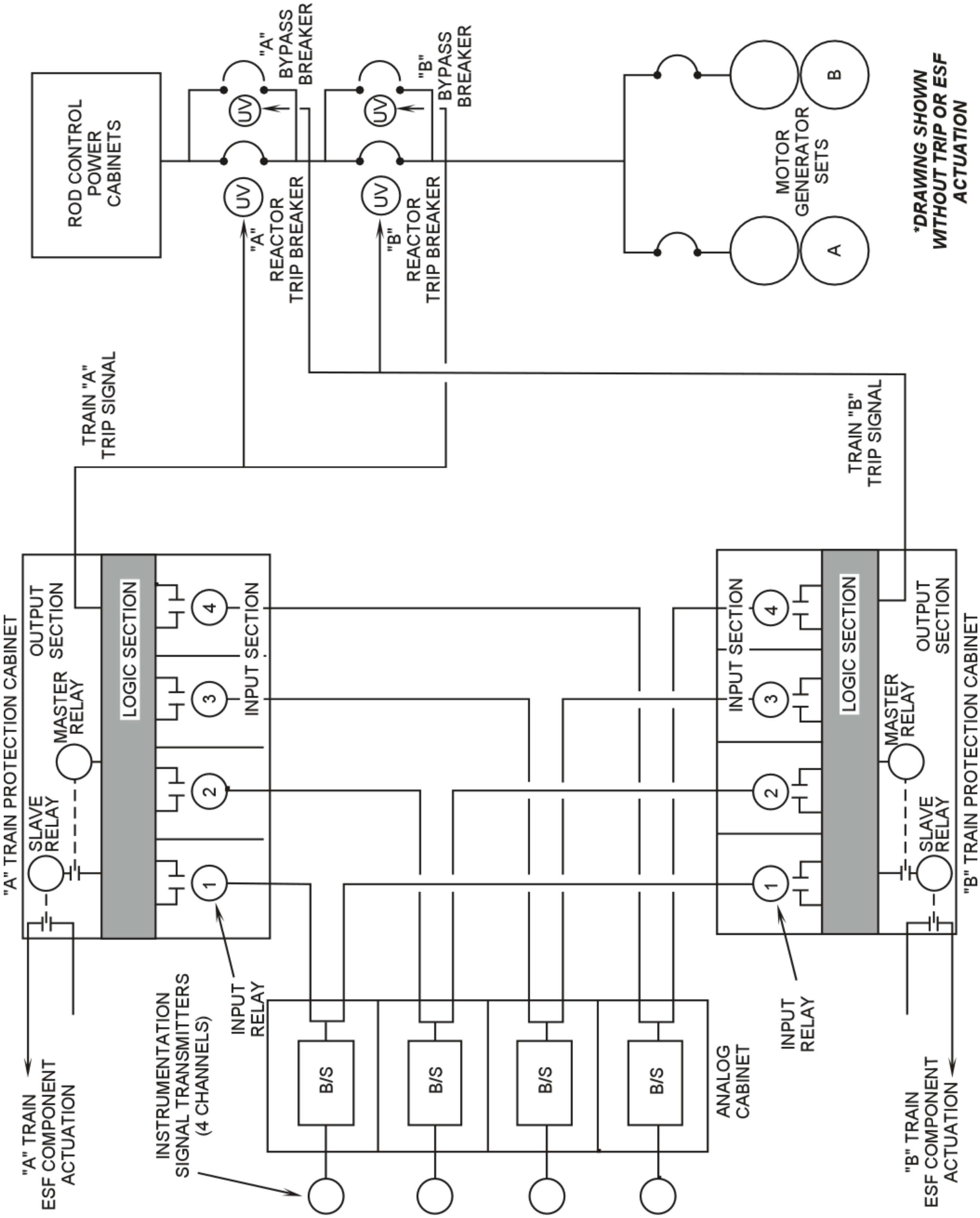

Figure 4.7-1 Solid State Protection System

This page intentionally blank

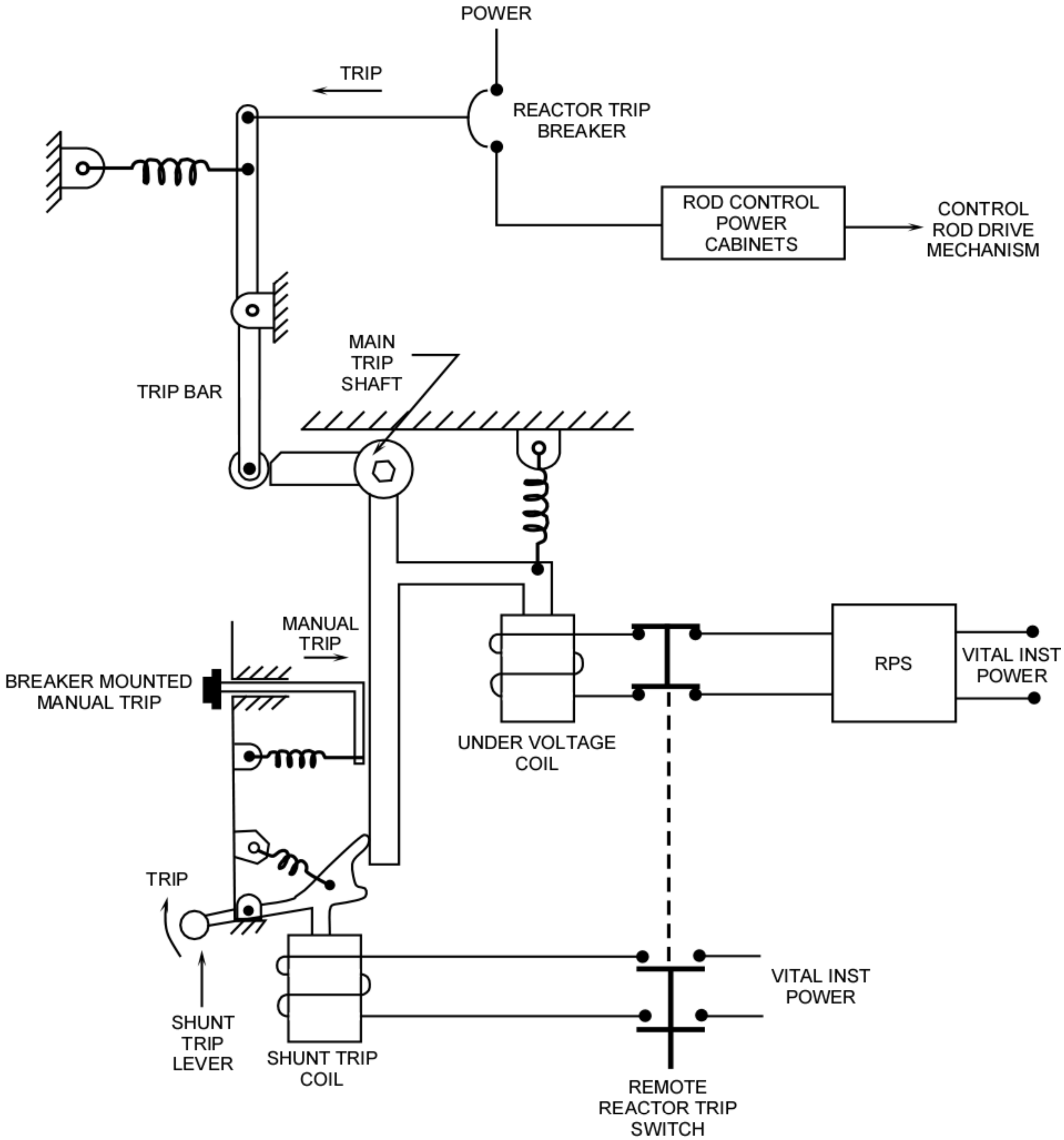

Figure 4.7-2 Reactor Trip Breaker

This page intentionally blank

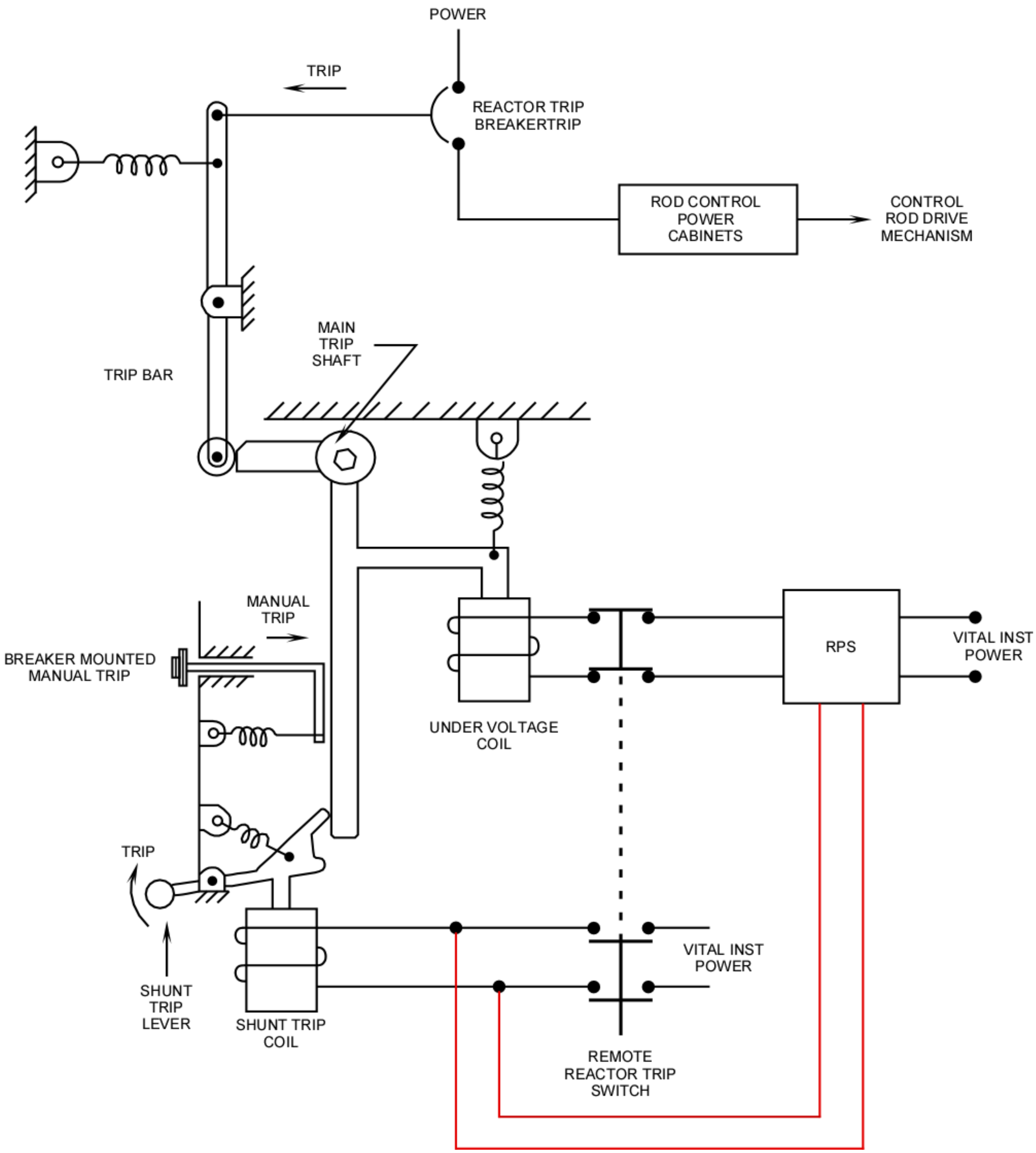

Figure 4.7-3 Reactor Trip Breaker Modification

This page intentionally blank

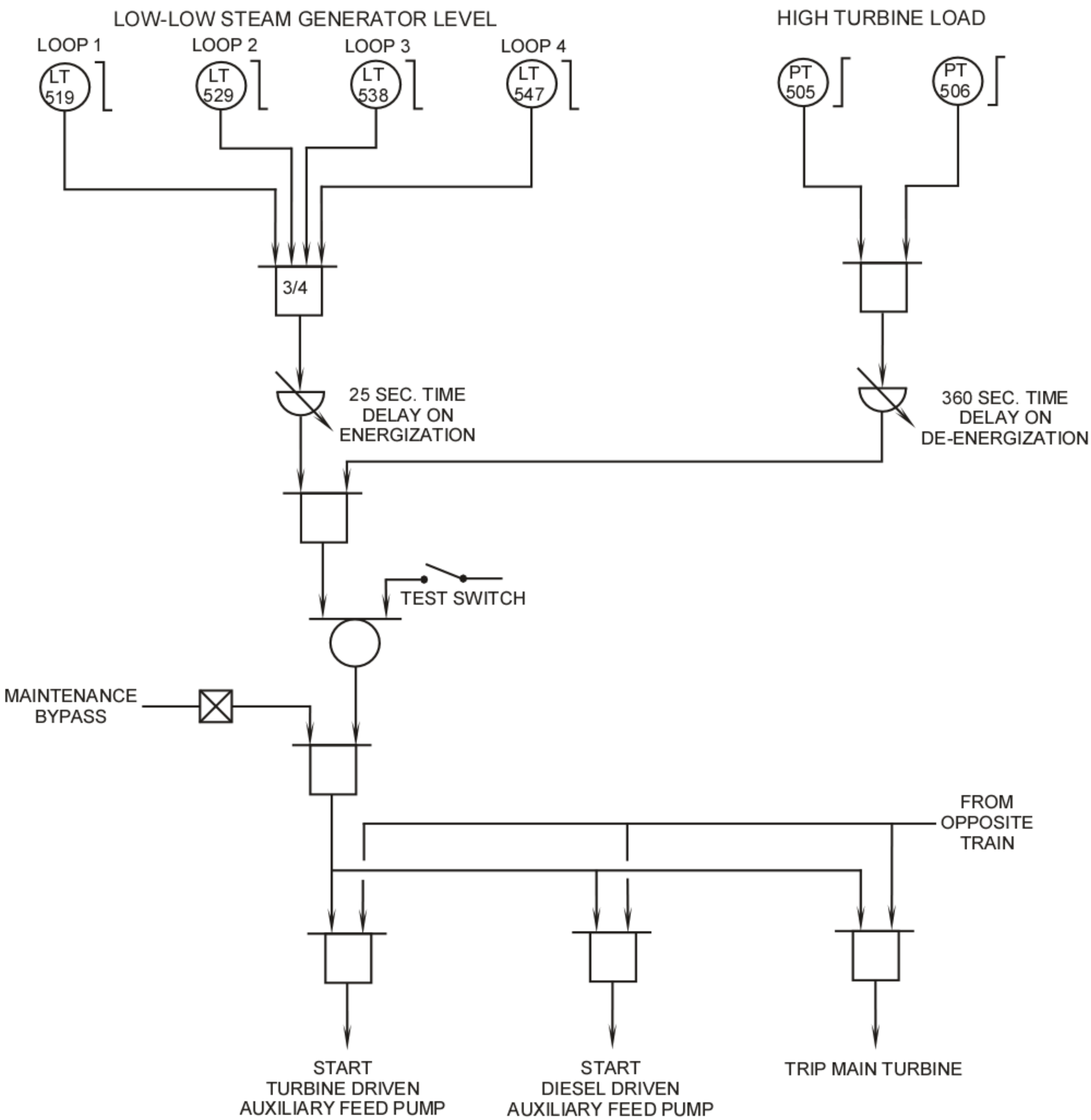

Figure 4.7-4 Trojan AMSAC Trip Circuit

This page intentionally blank

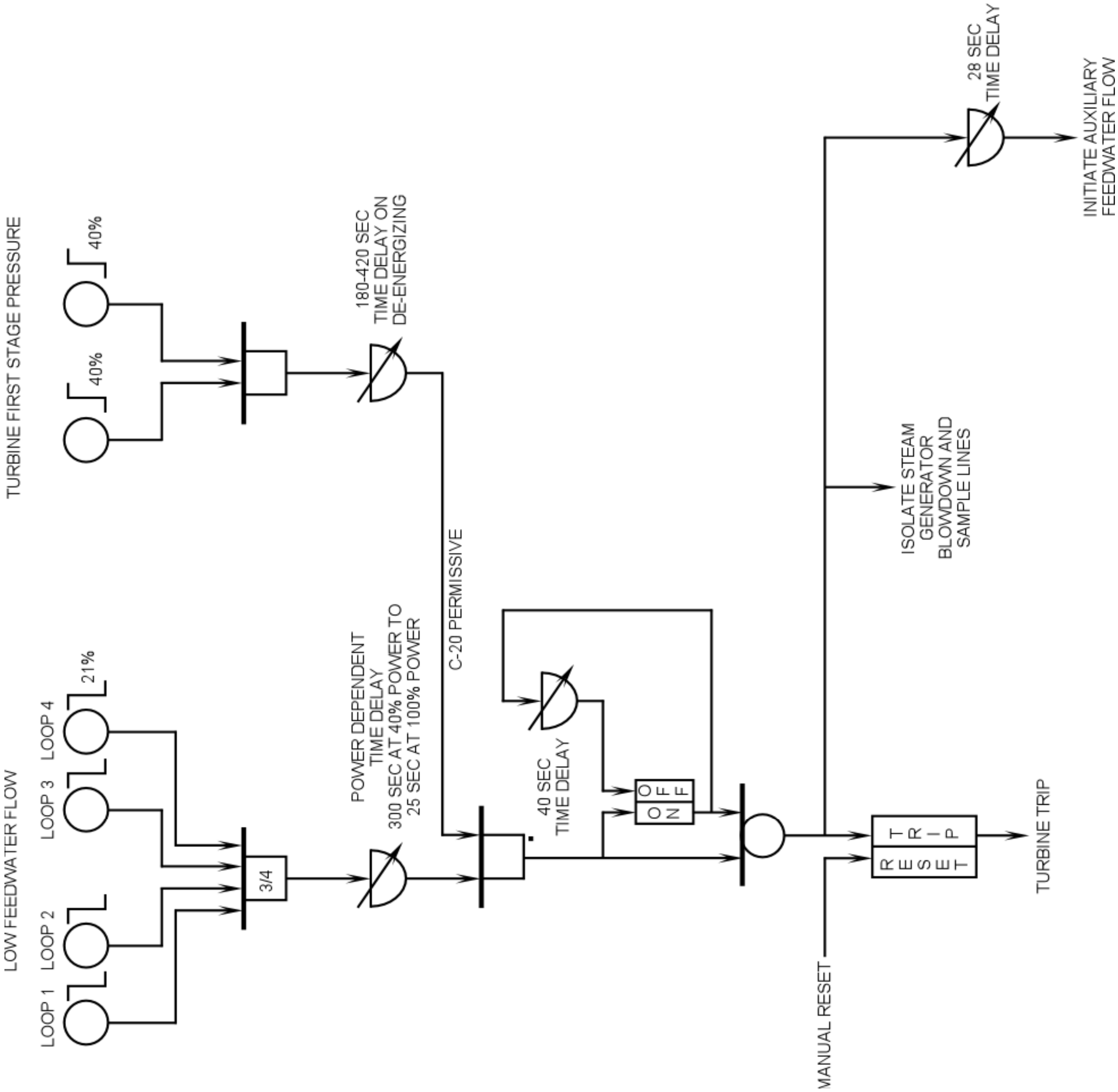

Figure 4.7-5 Indian Point Unit 3 AMSAC

This page intentionally blank

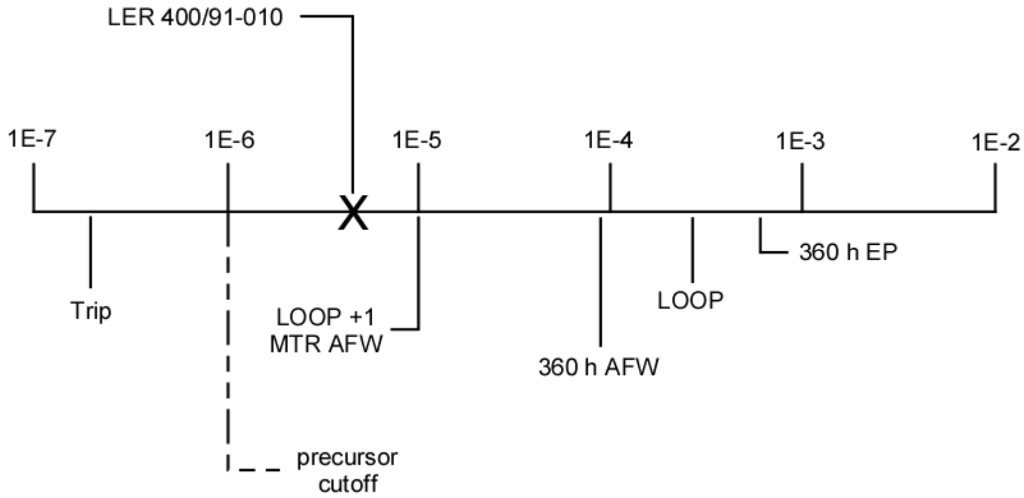

Figure 4.7-6(a) Relative Significance of Event Compared to Other Postulated Events at Harris 1

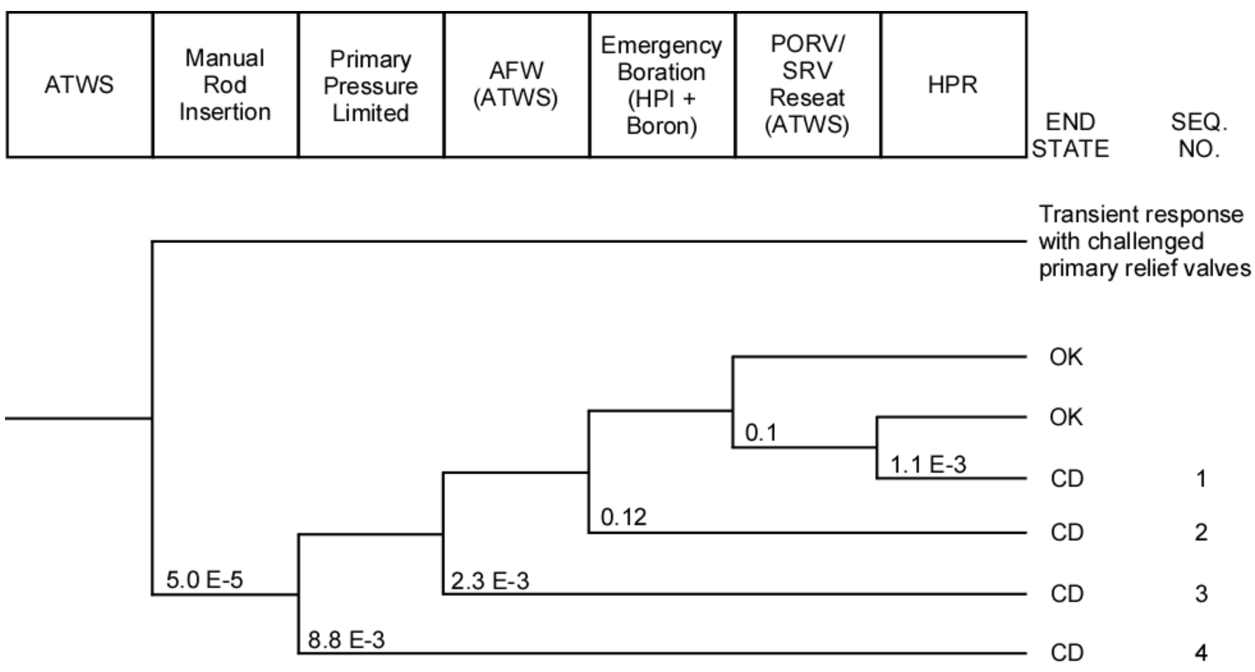

Figure 4.7-6(b) Model Used to Estimate the Conditional Core Damage Probability

This page intentionally blank