7.8 ATWS MITIGATION SYSTEM ACTUATION CIRCUITRY (AMSAC)

7.8.1 Description

7.8.1.1 System Description

The ATWS (Anticipated Transient Without Scram) Mitigation System Actuation Circuitry (AMSAC) provides a backup to the Reactor Trip System (RTS) and ESF Actuation System (ESFAS) for initiating turbine trip and auxiliary feedwater flow in the event an anticipated transient results (e.g., in the complete loss of main feedwater). The AMSAC is independent of and diverse from the RTS and ESFAS, with the exception of the final actuation devices, and is classified as control-grade equipment. It is a highly reliable, microprocessor-based, single-train system powered by a non-Class 1E source.

The AMSAC continuously monitors level in the steam generators, which is an anticipatory indication of a loss of heat sink, and initiates certain functions when the level drops below a predetermined setpoint for at least a preselected time and for three of the four steam generator levels. These initiated functions are tripping of the turbine, initiation of auxiliary feedwater, and isolation of steam-generator blowdown and sample lines.

The AMSAC is designed to be highly reliable, resistant to inadvertent actuation, and easily maintained. Reliability is assured through the use of internal redundancy and continual self-testing by the system. Inadvertent actuations are minimized through the use of internal redundancy and majority voting at the output stage of the system. The time delay on low steam generator level and the coincidence logic used also minimize inadvertent actuations.

The AMSAC automatically performs its actuations when above a preselected power level, which is determined using turbine steamline inlet pressure, and remains armed sufficiently long after that pressure drops below the setpoint to ensure that its function will

be performed in the event of a turbine trip.

7.8.1.2 Equipment Description

The AMSAC consists of a single train of equipment located in a seismically qualified cabinet.

The design of the AMSAC is based on the industry standard Intel multibus format, which permits the use of various readily available, widely used microprocessor cards on a common data bus for various functions.

The AMSAC consists of the following:

1. Steam generator level sensing - Measured with four existing differential pressure-type level transmitters for each of the main steam generators.

2. Turbine steamline inlet pressure - Measured with two existing pressure transmitters located in the steam supply line near the turbine.

3. System hardware - Consists of two primary systems: the Actuation Logic System (ALS) and the Test/Maintenance System (T/MS).

    a. Actuation Logic System

    The ALS monitors the analog inputs, performs the functional logic required, provides actuation outputs to trip the turbine and initiate auxiliary feedwater flow, and provides status information to the T/MS. The ALS consists of three groups of input/output (I/O) modules, three actuation logic processors (ALPs), two majority voting modules, and two output relay panels. The I/O modules provide

signal conditioning, isolation, and test features for interfacing the ALS and T/MS. Conditioned signals are sent to three identical ALPs for analog-to-digital conversion, setpoint comparison, and coincidence logic performance. Each of the ALPs performs identical logic calculations using the same inputs and derives component actuation demands, which are then sent to the majority voting modules. The majority voting modules perform a two-out-of-three vote on the ALP demand signals. These modules drive the relays providing outputs to the existing turbine trip and auxiliary feedwater initiation circuits.

b. Test/Maintenance System

The T/MS provides the AMSAC with automated and manual testing, as well as a maintenance mode. Automated testing is the continuously performed self-checking done by the system during normal operation. ALS status is monitored by the T/MS and sent to the plant computer and main control board. Manual testing of the system by the maintenance staff can be performed online to provide assurance that the ALS system is fully operational. The maintenance mode permits the maintenance staff, under administrative control, to modify channel setpoints, channel status, and timer values and to initiate channel calibration.

The T/MS consists of a test/maintenance processor, a digital-to-analog conversion board, a memory board, expansion boards, a self-health board, digital output modules, a test/

maintenance panel, and a portable terminal/printer.

4. Equipment Actuation

The output relay panels provide component actuation signals through isolation relays, which then drive the final actuation circuitry for initiation of auxiliary feedwater and for turbine trip. Existing actuation devices of the component are used.

7.8.1.3 Functional Performance Requirements

The AMSAC automatically initiates auxiliary feedwater, trips the turbine, and isolates steam generator blowdown and sampling lines. Analyses have shown that the most limiting ATWS event is either a loss of feedwater or a loss of load event without a reactor trip. Therefore, the AMSAC performs its mitigative actuations for the following reasons:

1. To ensure a secondary heat sink following an anticipated transient (ANS Condition II) without a reactor trip.

2. To limit core damage following an anticipated transient without a reactor trip.

3. To ensure that energy generated in the core is compatible with design limits to protect the reactor coolant pressure boundary by maintaining reactor coolant pressure to within ASME Stress Level C.

7.8.1.4 AMSAC Interlocks

A single interlock, designated as C-20, is provided to allow for automatic arming and blocking of the AMSAC. The system is blocked at sufficiently low reactor power levels when actions taken by the AMSAC following an ATWS need not be automatically initiated. Turbine steamline inlet pressure in a two-out-of-two logic scheme is

used for this permissive. Turbine steamline inlet pressure above the setpoint will automatically defeat any block, i.e., arm the AMSAC. Dropping below this setpoint will automatically block the AMSAC. Removal of the C-20 permissive is automatically delayed for a predetermined time. The operating status of the AMSAC is displayed on the main control board.

7.8.1.5 Steam Generator Level Sensor Arrangement

Steam generator level is determined by a differential pressure transmitter that measures the level drop in the steam generator. These steam generator level signals are used as input to the AMSAC and are isolated signals from the process protection cabinets routed through the control cabinets.

7.8.1.6 Turbine Impulse Chamber Pressure Arrangement

Turbine steamline inlet pressure is determined by a differential pressure transmitter that measures the pressure rise in the turbine. These pressure signals are used as input to AMSAC and are isolated signals from the process protection cabinets routed through the control cabinets.

7.8.1.7 Trip System

The differential pressure that is measured in the steam generator is used by the AMSAC to determine trip demand. Signal conditioning is performed on the transmitter output and used by each of the ALPs to derive a component actuation demand. If three of the four steam generators have a low level at a power level greater than the C-20 permissive, a trip demand signal is generated. This signal drives output relays to perform the necessary mitigative actions.

7.8.1.8 Isolation Devices

AMSAC is independent of the RTS and ESFAS. The AMSAC inputs that measure turbine steamline inlet pressure and narrow-range steam

generator water level are derived from existing transmitters and channels within the process protection system. Connections to these channels are made downstream of Class 1E isolation devices which are located within the process protection cabinets. These isolation devices ensure that the existing protection system continues to meet all applicable safety criteria by providing isolation. Buffering of the AMSAC outputs from safety-related final actuation device circuits is achieved through qualified relays. A credible fault occurring in the nonsafety-related AMSAC will not propagate through and degrade the RTS and ESFAS.

7.8.1.9 AMSAC Diversity from the Reactor Protection System

Equipment diverse from the RTS and ESFAS is used in the AMSAC to prevent common-mode failures that might affect the AMSAC and the RTS or ESFAS. The AMSAC is a digital, microprocessor-based system, with the exception of the analog steam generator level and turbine steamline inlet pressure transmitter inputs, whereas the reactor trip system utilizes an analog-based protection system. Also, where similar components are utilized for the same function in both AMSAC and the RTS, the components used in AMSAC are provided from a different manufacturer.

Common-mode failure of identical components in the analog portion of the RTS, resulting in the inability to generate a reactor trip signal, will not impact the ability of the digital AMSAC to generate the necessary mitigative actuations. Similarly, a postulated common-mode failure affecting similar components in ESFAS, affecting its ability to initiate auxiliary feedwater, and the same components in the AMSAC would impact the ability to automatically initiate auxiliary feedwater, but not the ability of the RTS to generate a reactor trip signal.

7.8.1.10 Power Supply

The AMSAC power supply is a non-Class 1E vital bus that is independent of RTS power supplies and backed by batteries

independent of the existing batteries which supply the RTS.

7.8.1.11 Environmental Variations

The AMSAC equipment is located in a controlled environment such that variations in ambient conditions are minimized. No AMSAC equipment is located inside containment. The transmitters (steam generator level and turbine steamline inlet pressure) that supply the input into AMSAC are located inside containment and the turbine building, respectively. The existing equipment inside containment is qualified.

7.8.1.12 Setpoints

The AMSAC makes use of two setpoints in the coincidence logic to determine if mitigative functions are required. Water level in each steam generator is sensed to determine if a loss of secondary heat sink is imminent. The low-level setpoint is selected so that a true lowering of the level will be detected by the system. The normal small variations in steam generator level will not result in a spurious AMSAC signal.

The C-20 permissive setpoint is selected to be consistent with ATWS investigations showing that mitigative actions performed by the AMSAC need not be automatically actuated below a certain power level. The maximum allowable value of the C-20 permissive setpoint is defined by these investigations.

To avoid inadvertent AMSAC actuation on the loss of one main feedwater pump, AMSAC actuation is delayed by a defined amount of time. This ensures that the reactor protection system will provide the first trip signal.

To ensure that the AMSAC remains armed sufficiently long to permit its function in the event of a turbine trip, the C-20 permissive is maintained for a preset time delay once the turbine steamline inlet pressure drops below the setpoint.

The setpoints and the capability for their modification in the AMSAC are under administrative control.

7.8.2 Analysis

7.8.2.1 Safety Classification/Safety-Related Interface

The AMSAC is not safety-related and therefore need not meet the requirements of IEEE 279-1971. The AMSAC has been implemented such that the RTS and ESFAS continue to meet all applicable safety-related criteria. The AMSAC is independent of the RTS and ESFAS. The isolation provided between the RTS and the AMSAC and between the ESFAS and the AMSAC by the isolator modules and the isolation relays ensures that applicable safety-related criteria are met for the RTS and the ESFAS.

7.8.2.2 Redundancy

System redundancy has not been provided. Since AMSAC is a backup nonsafety-related system to the redundant RPS, redundancy is not required. To ensure high system reliability, portions of the AMSAC have been implemented as internally redundant, such that a single failure of an input channel or ALP will neither actuate nor prevent actuation of the AMSAC.

7.8.2.3 Diversity from the Existing Trip System

Diverse equipment has been selected in order that common-cause failures affecting both the RTS and the AMSAC, or both the ESFAS and the AMSAC, will not render these systems inoperable simultaneously. A more detailed discussion of the diversity between the RTS and the AMSAC and between the ESFAS and the AMSAC is presented in Section 7.8.1.1.

7.8.2.4 Electrical Independence

From the sensor output up to the final actuation devices, the AMSAC

is electrically independent of the RTS and ESFAS. Isolation devices are provided to isolate the nonsafety AMSAC circuitry from the safety-related actuation circuits of the auxiliary feedwater system.

7.8.2.5 Physical Separation from the RTS and ESFAS

AMSAC must be and is physically separated from existing protection system hardware. AMSAC outputs are provided from separate relay panels within the cabinets. The two trains are separated within the AMSAC cabinet by a combination of metal barriers, conduit, and distance.

7.8.2.6 Environmental Qualification

Equipment related to the AMSAC is qualified to operate under conditions resulting from anticipated operational occurrences for the respective equipment location. The AMSAC equipment located outside containment in a mild environment follows the same design standard that currently exists for non-Class 1E control grade equipment.

7.8.2.7 Seismic Qualification

It is required that only the isolation devices comply with seismic qualification. The AMSAC output isolation device is qualified in accordance with a program that was developed to implement the requirements of IEEE Standard 344-1975, "IEEE Standard for Seismic Qualification of Class 1E Electrical Equipment for Nuclear Power Generating Stations."

7.8.2.8 Test, Maintenance, and Surveillance Quality Assurance

NRC Generic Letter 85-06, "Quality Assurance Guidance for ATWS Equipment That is not Safety-Related," requires quality assurance procedures commensurate with the nonsafety-related classification of the AMSAC. The quality controls for the AMSAC are, at a minimum,

consistent with existing plant procedures or practices for nonsafety-related equipment.

Design of the AMSAC followed procedures relating to equipment procurement, document control, and specification of system components, materials, and services. In addition, specifications also define quality assurance practices for inspections, examinations, storage, shipping, and tests as appropriate to a specific item or service.

A computer software verification program and a firmware validation program have been implemented commensurate with the nonsafety-related classification of the AMSAC to ensure that the system design requirements implemented with the use of software have been properly implemented and to ensure compliance with the system functional, performance, and interface requirements.

System testing is completed prior to installation and operation of the AMSAC, as part of the normal factory acceptance testing and validation program. Periodic testing is performed both automatically, through use of the system automatic self-checking capability, and manually, under administrative control via the AMSAC test/maintenance panel.

7.8.2.9 Power Supply

Power to the AMSAC is from a battery-backed, non-Class 1E vital bus independent of power supplies for the RTS and ESFAS. The station battery supplying power to the AMSAC is independent of those used for the RTS and ESFAS. The AMSAC is an energize-to-actuate system capable of performing its mitigative functions with a loss of offsite power.

7.8.2.10 Testability at Power

The AMSAC is testable at power. This testing is done via the system test/maintenance panel. The capability of the AMSAC to perform its

mitigative actuations is bypassed at a system level while in the test mode. Total system testing is performed as a set of three sequential, partial, overlapping tests. The first test checks the analog input portions of the AMSAC to verify accuracy. Each of the analog input modules is checked separately. The second test checks each ALP to verify that the appropriate coincidence logic is sent to the majority voter. Each ALP is tested separately. The last test exercises the majority voter and the integrity of the associated output relays. The majority voter and associated output relays are tested by exercising all possible input combinations to the majority voter. The integrity of each of the output relays is checked by confirming continuity of the relay coils without operating the relays. The capability to individually operate the output relays, confirm integrity of the associated field wiring, and operate the corresponding isolation relays and final actuation devices at plant shutdown is provided.

7.8.2.11 Inadvertent Actuation

The AMSAC has been designed such that the frequency of inadvertent actuations is minimized. This high reliability is ensured through use of three redundant ALPs and a majority voting module. A single failure in any of these modules will not result in a spurious AMSAC actuation. In addition, a three-out-of-four low steam generator level coincidence logic and a time delay have been selected to further minimize the potential for inadvertent actuations.

7.8.2.12 Maintenance Bypasses

The AMSAC is blocked at the system level during maintenance, repair, calibration, or test. While the system is blocked, the bypass condition is continuously indicated in the main control room.

7.8.2.13 Operating Bypasses

The AMSAC has been designed to allow for operational bypasses with inclusion of the C-20 permissive. Above the C-20 setpoint the

AMSAC is automatically unblocked (i.e., armed); below the setpoint the system is automatically blocked. The operating status of the AMSAC is continuously indicated in the main control room via an annunciator window.

7.8.2.14 Indication of Bypasses

Whenever the mitigative capabilities of the AMSAC are bypassed or deliberately rendered inoperable, this condition is continuously indicated in the main control room. In addition to the operating bypass, any manual maintenance bypass is indicated via the AMSAC general warning sent to the main control room.

7.8.2.15 Means for Bypassing

A permanently installed system bypass selector switch is provided to bypass the system. This is a two-position selector switch with "NORMAL" and "BYPASS" positions. At no time is it necessary to use any temporary means, such as installing jumpers or pulling fuses, to bypass the system.

7.8.2.16 Completion of Mitigative Actions Once Initiated

The AMSAC mitigative actions go to completion as long as the coincidence logic is satisfied and the time delay requirements are met. If the flow in the feedwater lines is reinitiated before the timer expires and the steam generator water level increases to above the low-low setpoint, then the coincidence logic will no longer be satisfied and the actuation signal will disappear. If the coincidence logic conditions are maintained for the duration of the time delay, then the mitigative actions go to completion. The auxiliary feedwater initiation signal is latched in at the component actuating devices, and the turbine trip is latched at the turbine electrohydraulic control system. Deliberate operator action is then necessary to terminate auxiliary feedwater flow, clear the turbine trip signal using the main control board turbine trip reset switch, and proceed with reopening of the turbine stop valves.

7.8.2.17 Manual Initiation

Manual initiation of the AMSAC is not provided. The capability to initiate the AMSAC mitigative functions manually, i.e., initiate auxiliary feedwater, trip the turbine, and isolate steam generator blowdown and sampling lines, exists at the main control board.

7.8.2.18 Information Readout

The AMSAC has been designed such that the operating and maintenance staffs have accurate, complete, and timely information pertinent to the status of the AMSAC. A system-level general warning alarm is indicated in the control room. Diagnostic capability exists from the test/maintenance panel to determine the cause of any unanticipated inoperability or deviation.

7.8.3 Compliance with Standards and Design Criteria

The AMSAC meets the applicable requirements of Part 50.62 of Title 10 of the Code of Federal Regulations and the quality assurance requirements of NRC Generic Letter 85-06. No other standards currently apply to the AMSAC.