7.3 ENGINEERED SAFETY FEATURES INSTRUMENTATION

7.3.1 Description

The Engineered Safety Features (ESF) Systems are actuated by redundant logic and coincidence networks similar to those used for reactor protection. Each network actuates a device that operates the associated ESF equipment, motor starters and valve operators. The channels are designed to combine redundant sensors, and independent circuitry, and coincident trip logic. Where possible, different but related parameter measurements are utilized. This ensures a safe and reliable system in which a single failure will not defeat the intended function. The action initiating sensors are listed in Table 7.3-1. The ESF Instrumentation System actuates (depending on the severity of the condition) the Safety Injection System (SIS), containment isolation, Containment Spray System (CSS) and the diesel generators.

Availability of control power to the ESF trip channels is continuously monitored. In general, the loss of instrument power to the sensors, instruments, or logic devices in the ESF instrumentation places that channel in the trip mode. An exception is the containment spray initiating channels which require instrument power for actuation.

The passive accumulators of the Emergency Core Cooling System (ECCS) do not require signal or power sources to perform their functions. The actuation of the active portion of the ECCS is from signals described in Table 7.2-1.

Containment spray operation is initiated by containment high-high pressure. Containment Spray Actuation Signal (CSAS) logic is shown on Figure 7.3-1. The containment pressure is sensed by four independent pressure detectors which are combined in a two-out-of-four logic network. The output signal provides two independent channels for containment spray actuation via the two

logic trains. Each CSAS channel initiates operation of a containment spray pump and associated valving.

In the event of a CSAS, the containment spray pumps would be operated from the normal source of power. If this is not available, or subsequently becomes unavailable, the power would be supplied by the emergency diesel generators.

Each spray system isolation valve is opened on a CSAS by a hi-hi containment pressure signal. Containment isolation backup is provided by check valves in the spray system piping.

The spray pump motor starting circuits and spray valve control circuits are provided with manual control switches in the control room. Each pump and isolation valve has test features to permit periodic operability testing of components and circuitry without causing interruption of the spray into the Containment Building.

The logic which initiates containment isolation is shown on Figure 7.3-1. There are four independent containment pressure detectors. Three of the pressure detectors are combined in a two-out-of-three logic to provide the signal for containment isolation for non-essential process lines if the high pressure setpoint is reached. This initiates Phase A containment isolation and safety injection. All four pressure detectors are combined in a two-out-of-four logic to provide the containment isolation signal for all penetrations (including those open to the containment atmosphere), except those required for operation of the ESF if the high-high pressure setpoint is reached. This initiates Phase B containment isolation, steam line isolation and containment spray.

A table of isolation valve schemes is given in Section 6.2. Air operated isolation valves will automatically go to their ESF position on loss of control air.

The design of the Control Air System precludes the total loss of control air to all systems and equipment. The control air systems are designed to provide a reliable supply of control air during normal and abnormal plant conditions, assuming a single failure in the system. See Section 9.3 for a detailed description of the system.

Isolation valves will be tested when the unit is off-line. The power supply to the Containment Isolation System (CIS) is the vital electrical supply described in Section 8.

Manual actuation of each channel may be accomplished from central control or local switches and individual valve control switches located in the Control Room for isolation valve operation.

Each valve has test features to permit periodic testing of components and circuitry without causing interruption of the containment isolation initiating signal.

The containment isolation signals provide the means of isolating the various pipes passing through the containment walls as required to prevent the release of radioactivity to the outside environment in the event of an accident. The signals for actuation of the containment isolation are given in Table 7.2-1 and Figure 7.3-1.

7.3.1.1 System Design

7.3.1.1.1 Engineered Safety Features Actuation Instrumentation Description

The ESF actuation circuitry and hardware layout are designed to maintain channel isolation up to and including the bistable operated logic relay similar to that of the reactor protection circuitry as discussed in Section 7.2. See Reference 1 for a complete description of the instrumentation.

7.3.1.1.2 Engineered Safety Features and Associated Systems' Actuation

Table 7.2-1 lists the ESF and associated systems' actuation signals.

7.3.1.1.3 Engineered Safety Features Vital Functions

The ESF actuation system automatically performs the following vital functions:

1. Starts operation of the SIS upon: a) low pressurizer pressure signals; b) high containment pressure signals; c) high differential steam pressure between steam lines; or d) high steam line flow signals with low-low T_{avg} or low steam line pressure.

2. Operates the containment isolation valves in non-essential process lines (Phase A Isolation) upon detection of high containment pressure signals.

3. Starts the CSS and operates the remaining containment isolation valves (Phase B Isolation) upon detection of high-high containment pressure.

4. Isolates all main steam isolation valves (MSIVs) on high steam flow coincident with low-low T_{avg} or low steam pressure or high-high containment pressure signals.

5. Safety injection signal will isolate the feedwater lines by closing all control valves (main and bypass valves), trip the main feedwater pumps and close the steam generator feedwater inlet stop valves, and actuate the Auxiliary Feedwater System. It also directly trips the turbine and the reactor.

7.3.1.1.4 Engineered Safety Features Calibration and Test

The ESF actuation channels are designed with sufficient redundancy to provide the capability for channel calibration and test during power operation. Except for containment spray actuation, removal of one actuation channel for test is accomplished by placing that channel in a tripped mode, i.e., a two-out-of-three matrix logic becomes a one-out-of-two matrix logic. Testing does not trip the system unless a trip condition occurs in a redundant channel.

Containment spray actuation channels (from containment pressure) are tested by removing the channel from service. Since 2/4 logic is used, 2/3 logic remains active during testing.

See Reference 1 for a description of analog and logic testing.

7.3.1.1.5 Feedwater Isolation

Any safety injection signal will isolate the main feedwater lines by closing all control valves, tripping the main feedwater pumps and closing the steam generator feedwater inlet stop valves.

7.3.1.1.6 Main Steam Isolation

Protection against a steam line break is provided by safety injection actuation, feedwater isolation to prevent excessive cooldown of the primary side, and main steam isolation to prevent uncontrolled blowdown of more than one steam generator. Closure of all MSIVs is initiated by high steam flow in 2 of 4 coincident with either low-low Tavg in 2 of 4 loops or low steam pressure in 2 of 4 lines, by 2 of 4 high-high containment pressure signals, or by 1 of 1 manual pushbuttons per loop. The automatic actuation system is designed to meet the requirements for protective systems as described in sections 7.1.2 and 7.2.1.

7.3.1.1.7 Indication

All transmitted signals (flow, pressure, temperature, etc.) which can cause actuation of the ESF are either indicated or recorded.

7.3.1.1.8 Engineered Safety Features Instrumentation

The following instrumentation ensures monitoring of the effective operation of the ESF.

Containment Pressure

Containment pressure is monitored by four taps, each connected to a pressure sensor, as shown on Figure 7.3-1. Each sensor provides an analog signal to its associated bistables which will trip at present signal values. These tripped bistables provide input to the protection logic circuits which, in turn, trip the relays to actuate the Safeguards System.

Three of the taps each have two bistables, the first of which is set to trip at the hi containment pressure value. When two of the three bistables are tripped, the logic circuits produce an "S-signal" and a "T-signal." The "S-signal" actuates the SIS while the "T-signal" initiates Phase A containment isolation. These first bistables are normally energized and become de-energized when tripped. Thus, a loss of power to two or more channels will produce a trip and initiate safety injection and containment isolation. However, the loss of one channel will neither cause nor prevent the above actions.

The fourth tap has only one bistable associated with its pressure sensor. This bistable, along with the second bistables associated with the other three channels, is set to trip at the hi-hi containment pressure value. When two of the four bistables are tripped, the logic circuits will initiate the containment spray and steam line isolation, and also produce a "P-signal." The "P-signal" initiates Phase B isolation. The bistables in this

second set are normally de-energized and become energized when tripped. Thus, momentary loss of power or voltage dip will not cause a spurious trip which would actuate the hi-hi containment signal. It should be noted that for containment spray the logic changes from 2/4 to 2/3 when a channel is placed on test.

Each channel is supplied with electrical power from one of four independent busses. These busses can draw power from the station's batteries through static inverters; a blackout or momentary loss of station power will not cause an interruption in the power supplied to the instruments.

Indicators and alarms are provided in the Control Room to inform the operator of system status and to guide actions taken during recovery operations.

Containment Radiation

There are two detectors, one monitoring containment particulate activity and the other monitoring containment gaseous activity. High radiation from either monitor will close containment ventilation isolation valves (Mode 6 only for particulate activity). These two monitors are not part of the Safeguards System and are not designed to meet the criteria of IEEE Standard 279.

Refueling Water Storage Tank Level

Unit 1 level instrumentation on the refueling water storage tank (RWST) consists of three channels. One channel provides a high level alarm to warn of an overflow condition, and a low level alarm. The second channel provides remote indication on the control panel, a low level backup alarm, a high alarm and a low-low level alarm. The third channel provides level indication.

Unit 2 level instrumentation consists of four channels. Two channels provide remote indication of high level, high level alarm signals and low level logic signals for semi-automatic switchover initiation. Two channels provide remote indication of level, low level alarm signals, low-low level alarm signals and low level logic signals for semi-automatic switchover initiation.

Emergency Core Cooling System Pump's Discharge Pressure

The discharge pressure for each of the safety injection pumps and the residual heat removal (RHR) pumps is indicated in one Control Room.

The common discharge header pressure for the charging pumps is indicated in the Control Room.

Pump Energization

The status (i.e., motor opened or closed) of each safeguards pump is indicated in the Control Room.

Valve Position

All ESF remote-operated valves have position indication on the control board to show valve limit position. Air-operated and solenoid-operated valves move in a preferred direction with the loss of air or power. Motor-operated valves fail as is upon loss of power.

The position of key valves in the ESF systems is also provided in a mimic fashion, according to safety function, on a vertical wall panel in the main Control Room.

Sump Instrumentation

The containment sump instrumentation consists of four level switches designed to operate in a post accident environment. The level light housings are located above any possible flooding level. The level switch lights and console lamp systems are located in the Control Room.

In addition to the above, the following local instrumentation is available.

1. RHR pumps' discharge pressure

2. Resi l heat exchanger exit temperatures

3. Containment spray test lines total flow

4. Safety injection test line pressure and flow

7.3.1.1.9 Instrumentation Used during a Loss-of-Coolant Accident (LOCA)

Instruments which are designed to function for various periods of time following a major LOCA are those which govern the operation of ESF. Pressurizer pressure and level and steam generator level sensors are located inside the containment because an equivalent signal cannot be obtained from a sensor loc a more isolated from the reactor. Steam flow is also measured inside the containment. Pressurizer pressure transmitters may be required to actuate ESF as a result of a LOCA.

It should be emphasized, however, that for the large loss-of-coolant incidents the initial suppression of the transient is independent of any detection or actuation signal because the water level will be restored to the core by the Passive Accumulator System.

The reactor vessel Level Microprocessor Instrumentation System utilizes three sets of differential pressure (d/p) cells. These cells measure the pressure drop from the bottom of the reactor vessel to the top of the reactor vessel, and from the top of the reactor vessel to the reactor coolant hot leg piping. The Differential Pressure Measuring System utilizes cells of differing ranges to cover different flow behavior with and without pump operation.

One pair of sensors provides an indication of the reactor vessel water level above the hot leg pipe when the reactor coolant pump

in the loop with the hot leg connection is not operating. When any reactor coolant pump is operating, the instrument reading will display "INVALID."

A second pair of sensors (narrow range) provides an indication of reactor vessel water level from the bottom to the top of the vessel when no pumps are operating. The instrument will also measure the reactor core and internal's pressure drop. When any reactor coolant pump is operating, the instrument will display "INVALID."

The third pair of sensors (wide range) provides an indication of reactor core, internals, and outlet nozzle pressure drop for any combination of operating reactor coolant pumps. Comparison of the measured pressure drop with the normal, single-phase pressure drop will provide an approximate indication of the relative void content or density of the circulating fluid. The RVLIS-86 stores four valves of expected reactor coolant void fraction. These expected values correspond to one through four RCPs running. The expected value of void fraction corresponding to the current pump operating status is displayed on the RVLIS-86 remote display panels. When all pumps are off, the indicator displays "INVALID". This instrument will monitor core conditions on a continuing basis.

To provide the required accuracy for water level measurement, temperature measurements of the reference legs are provided. These measurements, together with the existing reactor coolant temperature measurements, are used to compensate the d/p transducer outputs for differences in system temperature and reference leg temperature, particularly during the change in the environment inside the containment structure following an accident.

All pumps used for safety injection and containment spray are located outside the containment. The operation of the equipment can be verified by instrumentation that reads in the Control Room. This instrumentation will not be affected by the accident.

Depending upon the magnitude of the LOCA, information relative to the pressure of the Reactor Coolant System (RCS) will be useful to

THIS PAGE INTENTIONALLY LEFT BLANK

the operator to determine which pumps will be used for recirculation in the event of a small break. The discharge pressure of the charging pumps, as read on instrumentation outside the containment, will serve this purpose. The containment sump level and refueling water tank instrumentation will also provide information for evaluating the conditions necessary to initiate the recirculation mode of operation. See Section 6 for further details.

The RWST level instrumentation provides additional information to determine the relative size of a reactor coolant leak. Core recirculation and containment spray recirculation (if necessary) can be manually initiated before the RWST is empty.

Considerations have been given to all the instrumentation and information that will be necessary for the recovery time following a LOCA. Instrumentation external to the reactor containment, such as radioactivity monitoring equipment, will not be affected by this postulated incident and will be available to the operator.

7.3.1.1.10 Engineered Safety Features Control

All equipment required to keep the plant in a safe condition during the occurrences of safety injection, blackout, or both of these conditions, can be powered by three standby ac power systems per unit. The equipment is arranged such that safe shutdown can be achieved under all postulated abnormal conditions coincident with the loss of one diesel generator. Each unit has a separate and independent electrical system to provide power for Engineered Safeguards Systems.

Each diesel generator is provided with an independent loading Control System (Reference 2) which initiates the startup and/or loading of the diesel generators during the following plant conditions:

1. Safety injection only

2. Loss of all outside power (blackout)

3. Safety injection coincident with loss of all outside power

4. Safety injection coincident with undervoltage on the one 4 kV vital bus

During conditions of automatic startup and/or loading for all modes, the following criteria have been met in the Control System design:

1. Each vital bus control is independent of the other two.

2. Manual control of equipment is locked out until the automatic load sequencing is complete.

3. Safeguard actuation signals cannot be interrupted by any automatic device.

4. Manual initiation of the loading sequence is available to the operator.

5. Off-normal diesel conditions are alarmed in the Control Room.

6. Safety injection conditions take precedence over all other operating modes.

7. Diesel operating in a TEST mode at the occurrences of a blackout or safety injection, the diesel output breaker is automatically tripped open. The diesel is then reloaded according to prevailing conditions.

8. No sequential loading can occur until the diesel generator ACB is closed onto the bus.

9. Inadvertent tripping of the diesel generator output breaker is precluded by locking out the shutdown relay when a safeguard initiation signal is present.

7.3.1.1.10.1 Safety Injection Only

In this mode of operation, a safety injection signal initiates the following actions:

1. Start diesel generator units.

2. Lock out manual control of equipment circuit breakers until the loads are connected.

3. Connect all required accident loads.

Since outside power is available during this mode, the equipment not affected by the accident remains in service and required safeguards equipment is loaded immediately, except for the fan cooler units which are started for low speed operation as soon as they have coasted down from normal high speed operation (approximately 15 to 20 seconds). The diesel generators are started automatically so as to be available in the event they are subsequently required. They are not automatically connected to the vital busses. The operator may shut down the diesels when operation of the required equipment has been verified.

7.3.1.1.10.2 Blackout Only

In this mode of operation, a 70% undervoltage signal from each vital bus is combined in a two-out-of-three logic matrix per bus to develop a blackout loading signal for that bus. The blackout signal and the associated Control System perform the following functions on each bus:

1. Trip all 4160 V and selected 460 V vital bus breakers.

2. Start the diesel generator.

3. Lock ou manual control of bus loads until diesel generator loading is completed.

4. Connect the diesel generator to its bus.

5. Sequence the required blackout loads provided that an accident has not occurred and the diesel generator is ready to accept load.

During this mode of operation, manual control of individual circuit breakers is prevented until the automatic loading is completed. After a time delay has elapsed, the operator can manually reset the loading sequence signal and restore manual control.

7.3.1.1.10.3 Safety Injection Plus Blackout

This mode of operation differs from that of safety injection only in that circuit breakers of safety equipment cannot be closed until the diesel is ready to accept loads. These breakers are then closed sequentially.

The necessary logic required to recognize the existence of this mode is comprised of the coincidence of safety injection and blackout signals. This signal will trip selected 460 V and all 4 kV vital bus breakers.

Manual control of the individual loads is prevented by a time delay until diesel generator loading is complete. At that time, the loading sequence control can be reset and capability for manual control is restored.

The safeguards equipment required during an accident and blackout are automatically sequenced to start by the Safeguards Equipment Control (SEC) System. This is discussed further in Section 8.

The starting of the containment spray pumps requires a high-high containment pressure signal in addition to the SEC actuation signal. The containment spray pumps will normally start approximately 20 seconds following an accident. If the pumps do not start at the required sequence time, the SEC actuation signal will be delayed until the end of the loading sequence to prevent the spray pumps from starting when other equipment is required to start. The LOCA break sizes analyzed in Section 15 will result in the containment high-high pressure signal ("P" signal) before the SEC actuation signal calls upon the spray pumps to start. Break sizes which do not result in a "P" signal prior to the pump start initiation will result in a peak containment pressure at the end of the spray pump lockout period considerably lower than for the situations analyzed in Section 15. The postulated spray pump delay has no adverse effect on the safety of the plant and is not a controlling factor relative to maximum containment pressure design analyses.

The topics discussed in NUREG-0138 were addressed in a meeting with USNRC Region 1, Inspection and Enforcement personnel, prior to the startup of Salem Unit 1. The meeting resulted in a modification to the LOCA Emergency Instruction which requires the plant operating personnel to restart LOCA loads in the event of a loss of offsite power subsequent to reset of the safety injection signal. This procedure change is applicable to Unit 2 and it adequately addresses the positions taken by the NRC in NUREG-0138.

7.3.1.1.10.4 Safety Injection Plus One 4 kV Vital Bus Undervoltage

In this mode, the bus undervoltage signal is derived from the same group of relays which are used for the blackout signal logic matrices.

If an accident were to occur in coincidence with a single bus undervoltage condition, the following functions are performed by the controller:

1. Start the diesel on the affected bus.

2. Trip all vital bus equipment breakers.

3. Sequence the accident loads when the diesel is ready for loading.

4. Lock out manual control of breakers on the affected bus until diesel generator loading is complete.

7.3.1.1.10.5 Sustained Degraded Vital Bus Voltage (Degraded Grid)

The safeguards controllers also receive 95.1-percent (94.6% by technical specifications, the difference is relay calibration range) undervoltage signals from their respective vital buses through a 13-second time delay relay in order to provide a two-out-of-three logic intelligence. Upon completion of the logic, the affected vital bus is separated from the offsite source and loaded onto its associated emergency diesel generator. The loading sequence is identical to that of the blackout sequence.

7.3.1.1.10.6 Tests and Inspections

The Emergency Power Control System is provided with means to:

1. Check the operational capability of each input sensor during reactor operation,

2. Check that the logic combinations of input signals result in proper logic outputs or control system actions for each mode of operation,

3. Permit any one sensor to be maintained, tested or calibrated during power operation without initiating system action, and

4. Assure that when tests are completed the system is returned to its proper operational state.

7.3.1.2 Design Bases

7.3.1.2.1 General Design Criteria

Criterion: Protection systems shall be provided for sensing accident situations and initiating the operation of necessary ESF.

THIS PAGE INTENTIONALLY BLANK

The ESF instrumentation monitors parameters to detect failures and to initiate ESF equipment operation.

The ESF instrumentation measures temperatures, pressures, flows, levels in the RCS Steam System, Reactor Containment and Auxiliary Systems. It actuates the ESF and monitors their operation. Process variables required on a continuous basis for the startup, operation, and shutdown of the unit are indicated or recorded and controlled from the Control Room. The quantity and types of process instrumentation provided ensure safe and orderly operation of all systems and processes over the full operating range of the plant.

Certain controls and indicators which require a minimum of operator attention, or are only in use intermittently, are located on local control panels near the equipment to be controlled. Monitoring of the alarms of such control systems is provided in the Control Room. Design criteria for redundancy, separation and diversity are essentially the same as those used for the Protection System, and described in Sections 7.1, 7.2 and Section 8.

7.3.1.2.2 Environmental Capability

The ESF instrumentation equipment inside the containment is designed to operate under the accident environment of a steam-air mixture and radiation.

Electrical equipment for the ESF is located inside the containment and in the Auxiliary Building. Table 7.3-2 is a listing of the equipment inside the containment which is required for post-LOCA operation and indicates how long the equipment is required to function as well as specifying which components require qualification testing.

Failure of the equipment in Table 7.3-2 after the specified time will not increase the severity or consequence of the accident.

The reactor protection control and instrumentation equipment and electrical equipment for ESF located in the Auxiliary Building will operate in a normal ambient environment following a major LOCA.

7.3.2 System Evaluation

Redundant instrumentation has been provided for all inputs to the protective systems and vital control circuits. Where wide process variable ranges and precise control are required, both wide range and narrow range instrumentation are provided. Instrumentation components are selected from standard commercially available products with proven operating reliability. The instrument power to electrical and electronic instrumentation required for safe and reliable operation is supplied from the four instrument busses which can be energized from the diesel generator sources.

The Engineered Safeguards Initiation, Control, and Power Supply Systems are designed so that no single fault in components, units, channels or sensors will prevent ESF operation. The timing of initiation and startup of the ESF is such as to provide conservative protection.

The wiring is grouped so that no single fault or failure, including either an open or shorted circuit, will negate ESF operation. Wiring for redundant circuits is protected and routed independently so that damage to any one path will not prevent the protective action.

The detailed design incorporates the following characteristics in order to counteract faults resulting in loss of power:

1. Redundant components are powered from separate busses,

2. The 125 V dc and 110 V ac power busses used are discussed in detail in Section 8,

3. The 4160 V and 460 V systems are discussed in Section 8,

4. The starting and loading of diesel generators is described in Section 7.3.1.1.10.

7.3.2.1 Pressurizer Pressure

Credible accident conditions requiring emergency core cooling would involve low pressurizer pressure. The present design for emergency core cooling is accomplished by the SIS actuation from primary system variables. Actuation is initiated by low pressurizer pressure.

Pressurizer pressure is sensed by fast response pressure transmitters. An overall 1-second pressure channel response time, as used, is more than adequate to cover the response characteristics of the tripping channels.

Instrument delays are small in comparison with the computed lag in pressurizer pressure, which lags behind the reactor coolant pressure during blowdown.

A safety injection block switch is provided to permit the primary system to be depressurized, such as for refueling operations without actuation of the SIS. This manual block switch will be interlocked with pressurizer pressure in such a way that the blocking action will automatically be removed as operating pressure is approached. If two-out-of-three pressure signals are above this preset pressure, blocking action cannot be initiated. The block condition will be indicated by a status light in the Control Room.

7.3.2.2 Motor and Valve Control

For starting pump and fan motors, the control relays are energized to energize the closing coil on the circuit breaker or the motor starter. When motor starters are used the starter operating coil

will be supplied by power from the same source as the subject motor. When circuit breakers are used for motor control the circuit breakers close and trip coils will be supplied by power from a 125 V dc battery bus.

For valve motor control, the control relay causes the coil on the main contactor for the closing circuit to be energized.

Air-actuated containment isolation valves are spring loaded to close upon loss of air pressure.

7.3.2.3 Manual Control of Engineered Safety Features

Manual control of ESF equipment from the main control console is achieved through the use of a 28 V dc logic interface system.

The manual control system is comprised of four groups of logic cabinets, terminal cabinets, and wiring to the main control console. The console contains the back-lighted push-button stations used to initiate a control action. A momentary contact energizes the relays in the logic cabinets, which in turn cause the desired system action in the primary control circuit (115 V AC or 125 V DC). The output contacts of the logic relays are wired to the terminal cabinets and then out to the field equipment control centers.

Power for logic relays is provided by the two 28 V batteries. This is the supply voltage which appears across the contacts of the console pushbuttons. Wiring between the console and the logic cabinets consists of teflon insulated plug-in cables.

This system is used to manually initiate protective functions such as reactor trip, containment isolation, and containment spray. IEEE Standard 279-1971, Paragraph 4.17, is applicable to these functions. The 28 V control system meets the requirements of Paragraph 4.17. All automatic operation of the ESF equipment does not require any action in the 28 V circuitry.

7.3.2.4 Testing

The method of periodic testing of ESF instrumentation, control equipment, and ESF actuator testing is discussed below.

The discussions of system testability in Section 7.2 are applicable to the sensors, analog circuitry, and logic trains of the ESF Actuation System. The following information describes those areas in which the testing provisions differ from those for the Reactor Trip System.

The ESF Systems are tested to provide assurance that the systems will operate as designed and will be available to function properly in the unlikely event of an accident and/or loss of offsite power. The testing program includes:

1. Prior to initial plant operations, ESF System tests will be conducted.

2. Subsequent to initial startup, ESF System tests will be conducted during each regularly scheduled refueling outage.

3. During online operation of the reactor, the ESF analog and logic circuitry will be tested. In addition, essentially all of the ESF actuators will be tested. The remaining few final actuators whose operation is incompatible with online plant operation will be partially tested.

4. During normal operation of testable final actuation devices, the ESF Systems will be tested by manual initiation.

During reactor operation the basis for ESF Actuation System acceptability will be the successful completion of the overlapping tests performed on the Reactor Trip and the ESF Actuation Systems.

Analog checks verify operability of the sensors. Analog checks and tests verify the operability of the analog circuitry from the input of these circuits up to and including the logic input relays. Solid state logic testing checks the digital signal path from the logic input relay contacts through the logic matrices and master relays and performs continuity tests on the coils of the output slave relays; final actuator testing operates the output slave relays and verifies operability of those devices which require safeguards actuation, and which can be tested without causing plant upset. A continuity check is performed on the actuators of the untestable devices. Operation of the final devices is confirmed by control board indication and visual observation of the devices.

Maintenance checks (performed during regularly scheduled refueling outages), such as resistance to ground or signal cables in radiation environments, are based on qualification test data which identify acceptable radiation, thermal degradation, etc.

Considered in the design are:

1. Testing shall minimize the potential for accidental shutdown of the unit or initiation of emergency core cooling.

2. Test circuitry shall be designed to maintain overall reliability of the Engineered Safeguards Systems.

The operation of the ESF includes function of both the Solid State Protection System (SSPS) and the Safeguards Equipment Controller. The test provision for the SSPS is described below.

Description of Initiation Circuitry

Initiating relays are provided for the following systems or functions in each of the two trains of the SSPS:

1. Safety Injection

2. Containment Isolation Phase A

3. Containment Isolation Phase B

4. Containment Spray

* 5. Containment Ventilation Isolation

6. Main Steam Line Isolation

7. Main Feedwater Line Isolation

8. Safeguards Equipment Control (one for each diesel generator unit)

The output of the initiation circuits each consists of a master relay which drives slave relays for contact multiplication. The logic, master, and slave relays are mounted in cabinets designated Train A and Train B, respectively, for the redundant counterparts. The slave relay circuits operate some circuit breakers, motor-operated valves and solenoid-operated valves.

* NOTE: For Containment Ventilation Isolation from a RMS input, the initiating relays drive the slave relays directly. The logic circuits and master are not used for this function.

Actuator Testing

After testing of the initiation circuits in the SSPS and SEC has been accomplished, the SSPS master relays can be reset for testing of the slave relays and the devices controlled by their contacts. By operation of these relays one at a time, all breakers and valves that can be operated online are tested.

Breakers and valves are assigned to the slave relays such that no undesired effect on plant operation can occur. Controls mounted in a Solid State Protection Test Panel are used for actuator testing. Separate panels are used for the A and B Trains. A four-position selector switch permitting rotation in one direction

only is used to test all SSPS output relays. Turning the switch to the first-position blocks those outputs which cannot be tested with the plant at power. This blocking is accomplished by latch-type test relays in the test panel. For those outputs where blocking is not required, this position is not used.

When the switch is moved to the second position, the output relay is activated. For those circuits with no blocking, the field devices function and are tested. For those circuits that are blocked, the test relay places a built-in "press-to-test" indicator light in series with the field device. Due to the low current, the field device does not operate. For normally closed output relay contacts, the test relay switches a bypass contact around the output relay contact. Current flow is determined by reading the voltage drop across small resistors in series with the normal and bypass contacts (maximum drop = 1 V).

Position 3 resets the output relay. The test lights or resistors are used to verify contact resetting. Final Position 4 resets the test relay. Again, the test lights or resistors verify that the test relay has reset. Whenever a test switch is out of Position 4 or a test relay is latched, an SSPS test alarm is activated in the Control Room.

The method of using a four-position test switch and lights or resistors for verifying field device continuity permits testing without activating the field device and verifies that the system has been reset and is in the same state as before testing. Depressing the test light lens holder breaks the normal circuit and makes up a test circuit such that the lamp can be checked instantly.

Administratively, only one test switch is operated at a time so only one SSPS output relay is tested.

During output testing, close communication between the main Control Room operator and the man at the test panel is maintained.

Prior to operating a slave relay, the operator in the main Control Room assures that plant conditions will permit operation of the equipment that will be actuated by the relay. After the tester has actuated a slave relay the main Control Room operator observes that all equipment has operated properly. Prepared check lists are used to verify proper operation and keep a permanent record of tests. By means of the procedure outlined above, all equipment actuated by Engineered Safeguard System initiation circuits (with the following list of exceptions) is operated by the test circuitry:

1. Feedwater Isolation Valves

2. Main Steam Isolation Valves

3. Control Air Isolation Valves

4. Turbine Trips

5. Steam Generator Feedwater Pump Turbine Trip

6. Steam Generator Feedwater Pump Stop Valves

7. Reactor Coolant Pump Trip

8. Auxiliary Feedwater Pumps

9. Generator Trip

10. Safety Injection System Valves ISJ1, 1SJ2, 1SJ4, 1SJ5, 1SJI2, 1SJ13

11. Chemical and Volume Control System Valves 1CV40, ICV41, 1CV68, 1CV69, 1CV116, 1CV284, ICV7

12. Reactor Coolant Pump Seal and Thermal Barrier Cooling Valves 1CC117, 1CC118, 1CC131, 1CC136, 1CC187, 1CC190

13. Containment ventilation isolation: VC1, VC4, VC5 and VC6. There is no test circuit for the RMS input function.

The method described provides capability for checking from the process signal to the logic cabinets and from there to the individual field equipment including all field cabling actually used in the circuitry. For those devices whose operation could have an effect on plant stability, the procedure provides for checking from the process signal to the logic rack and continuity determination for output cables and field devices; however, the actuated equipment will be manually initiated as plant conditions permit.

The SEC units have the following test capability during power operation:

1. Check the operational capability of each bus undervoltage sensor and its input to the logic.

2. Check the operational capability of the LOCA signal, "S", from the SSPS logics.

3. Check that the logic combinations of input signals result in proper operation of the various functions, including automatic load sequencing, without actuation of any motors and a verification of the timed loading sequence.

4. Check the output relay capability to actuate the driven equipment.

The SEC units can also be checked for complete system operability from sensor to actuated equipment during plant shutdowns.

Reactor Trip System and ESF actuation system response time tests are required by and will be performed in accordance with the Technical Specifications.

7.3.2.5 Containment Flooding Analysis

The analyzed flood level within the containment following a major LOCA is set at Elevation 84 feet-0 inch (PS Datum). Table 7.3-3 lists all electrical components which are in the containment at or below Elevation 84 feet-0 inch and may be subjected to the effects of flooding. This list includes both safety-related and non-safety-related components and distinguishes between vital circuit (Class 1E) and non-vital circuit association. In addition there are some temperature elements which were not listed which may become flooded. These devices, however, do not perform a safety function, but are used for computer or annunciator alarms and will not have any effect on vital circuits or the safe operation of the plant following a LOCA.

Safety Significance

An analysis has been performed on the safety significance of the failure consequences of vital circuits due to postulated flooding. Submerged circuit components were examined for function and whether the function was required for the accident and performed prior to flooding. Tables 7.3-4, 7.3-5, 7.3-6 and 7.3-7 present the results in tabular form of the detailed analysis for 125 V dc circuits, 115 V ac circuits, 230 ac control center circuits and junction/terminal boxes, respectively. A detailed analysis of non-vital circuits is not required since their failure or improper operation will not affect the safety functions necessary for a LOCA incident.

The analysis demonstrates that the safety functions required for an accident will be performed. Containment isolation and accumulator pressure monitoring were found to be the major safety functions required and were not adversely affected by the flooding before the functions were performed.

Air-operated containment isolation valves required to close on an isolation signal are signaled to close prior to significant flooding and, except for 11, 12, 21 and 22CA330, close upon loss of power. In general, the flooding could cause short circuits, thereby tripping the control circuit breaker open and assuring that the safety function is performed. The CA330's are on the control air system supply headers, and fail-as-is on loss of vital DC power. They are located outside containment, and are above the maximum calculated containment flooding elevation. Motor-operated isolation valves also perform their function prior to flooding.

Indication of isolation valve position has been determined not to be of safety significance because the valves will have performed their function prior to flooding, and the closed status of the valves will be indicated before flooding can cause a trip of the circuit breaker and subsequent loss of the indication. If this occurs, alarms are provided to indicate loss of the control circuit. The circuitry design assures that loss of power would not result in loss of the containment isolation function. The failure of isolation valve indication resulting from flooding is therefore considered to be of no safety significance.

The accumulator pressure monitoring function will be available for the five minutes that it is required. The instruments are located at approximately Elevation 82 feet and will not become flooded until after they have performed their function.

The loss or improper operation of other instrumentation will not affect the operator's response to post accident conditions since they are neither required for the accident nor for post accident monitoring.

Effect on Class 1E Sources

Class 1E electrical power sources will not be adversely affected by the flooding of individual electrical circuits because of the circuit protection provided. Circuit protection for those items affected by the flooding is indicated in the tables for each circuit analysis.

Each 125 V dc circuit is protected by Class 1E, 15 amp circuit breakers which will trip open if short circuits are caused by the flooding of components in the containment. Power to the entire circuit would be lost. All components on the if their loss was acceptable.

Each 115 V ac circuit providing power to the process group racks and protection racks is also protected by Class 1E, 15 amp circuit breakers. However, in this case the entire circuit will not be lost due to flooding of components in part of the circuits. Each individual process or protection control/indication loop is provided with its own fuse protected power supply. The development of faults from flooding of components in the loop would blow the fuses and thereby isolate that portion of the circuit. Other functions powered from that particular circuit would not be affected.

In the analysis of 115 V ac circuits only those devices which would become submerged were examined as to function and need. Non-submerged components of the circuit will not be affected by the flooding. In the case of submerged devices in the 115 V ac circuit, it may be possible that total loss of control power will not occur, and that some control loops would provide anomalous indication or control. This has been examined and those devices which are required to operate properly do so for the required time period prior to submergence. Once submerged their functions are not required, and any improper operation would not be detrimental to the necessary safety functions following a LOCA.

Each 230 V motor control center circuit is provided with Class 1E circuit breakers. The control circuit power developed from a 230/115 V transformer is protected by fuses. Any isolation valves will have performed their function prior to becoming submerged. The reactor nozzle support vent fans are tripped during an accident. These power circuits are protected during

flooding conditions since voltage to the devices is removed by open motor starter contacts.

Design Changes

During the course of the review two instances were discovered which required a redesign to assure that the Emergency Core Cooling Systems can be operated effectively. They are described below:

1. Position interlock circuits for valves 1SJ67 and 1SJ68, although not flooded, were found to be on 125 V dc circuits which are affected by the flooding of other components. The position interlock circuit of 1SJ67 was on circuit 13 of the 1CCDC distribution cabinet and the position interlock circuit of 1SJ68 was on circuit 13 of the 1AADC distribution cabinet. Coincident flooding of components in portions of the circuits could trip the circuit breakers, thereby losing the interlock capability for opening 11SJ45 and 12SJ45. The power circuit for the 1SJ67 and 1SJ68 position interlocks was changed to circuits which cannot be affected by flooding.

2. The containment sump level instruments provide backup indication for initiating the recirculation phase of an accident and are above the flood level. However, two junction boxes, JN106 and JN108, used for the routing of the indication circuits, were located below the flood level. This situation could have caused anomalous indication to the operator and possibly affected his response to accident conditions. These two junction boxes were raised above the flood level.

In summary, with incorporation of the design changes, the entire analysis demonstrates that flooding within the containment will not adversely affect the safe operation of the plant following a

LOCA even though a number of vital circuits and non-vital circuits could be lost. The necessary safety functions will be performed.

7.3.2.6 Single Failure of Components

There are no single electrically operated fluid system components whose failure within the single failure criterion could result in the loss of capability of the Emergency Core Cooling System (ECCS) to perform its safety function. In order to achieve this, design changes were incorporated for certain manually controlled electrically operated valves. These changes are illustrated for typical valves on Figures 7.3-2, 7.3-3 and 7.3-4 and are described below.

Figure 7.3-2 illustrates the design provided for valves which have motive power "locked out" at the 230 V motor limit switches which provide redundant position indication as described in Section 7.6.2. All valves with this design are provided with a separate 125 V dc supply to provide power for control board position indication which would normally be unavailable due to the "power lockout."

Figure 7.3-3 illustrates the design provided for valves whose control power can be restored from the Control Room. The design incorporates a switch which isolates the operating coil of the motor starter which could cause spurious movement to the undesirable valve position. The switch is monitored by a light which would indicate failure of the switch to provide isolation, and by a separate light which gives positive indication that the motor is "locked out." Similar to the other valves previously described, these valves are provided with a separate 125 V dc supply for control board position indicating lights.

Figure 7.3-4 illustrates the design which provides the same design functions as Figure 7.3-3. The additional interposing relay 95/C, 95/O and aux. relay 43x are utilized due to the large in rush current for valves with size 3 starters. This is to ensure that sufficient control voltage is available to 9/C and 9/O starter coils during a degraded grid voltage condition.

7.3.2.7 Electrical Interlocks

Electrical interlocks are provided in the control circuits of several redundant ECCS valves. These interlocks assure that the proper sequence of operations occurs when switching to the

THIS PAGE INTENTIONALLY LEFT BLANK

recirculation phase of a LOCA. The interlocks also serve to prevent unacceptable system lineups during normal plant operations. All of the interlocks use redundant devices to prevent single failures from either defeating the ECCS safety function, or the operational restrictions during normal power operation. In addition to the interlock circuitry, some of the valves are provided with control "power lockout" to meet other criteria and are described below along with an assessment of the effects of failures in the circuits.

Valves 1CV40 and 1CV41

These valves are located in the normal suction line to the charging pumps. The closing of these valves requires opening of either 1SJ1 or 1SJ2 (charging pump suction lines from the RWST) to assure that the charging pumps do not lose suction. The normal operation of the interlocks requires 1SJ1 or 1SJ2 to be fully open prior to initiating closure of the 1CV40 and 1CV41 valves. If either interlock were to fail in the direction allowing premature closure of 1CV40 or 1CV41 during a LOCA, suction to charging pumps would not be lost since 1SJ1 and 1SJ2 would be opening at the same time. This simultaneous operation of all four valves occurs since "S" signals from the plant Protection System would be transmitted to the valve control circuits simultaneously. The devices used to develop the interlock circuits are redundant. If either interlock were to fail in the direction which would prevent closure of the 1CV40 or 1CV41 valves, the redundant interlock would function to close the valves.

Valves 11RH4 and 12RH4

These valves are located in the suction lines to the No. 11 and 12 RHR pumps, respectively. The opening of each valve is enabled by the closed condition of its respective containment sump isolation valve (11SJ44 interlocks 11RH4 and 12SJ44 interlocks 12RH4). The normal status of 11RH4 and 12RH4 is "open" and ready for the injection phase of a LOCA. The interlocks are arranged on a "Train" basis so that no possible interconnection of the interlocks can occur. A failure of either interlock would affect only the opening circuit of the RH4 valve associated with that interlock. The required safety function of the RH4 valves is to be closed for Unit 1 and closed after the SJ44 valves are full open for Unit 2 when initiating the recirculation phase of a LOCA. The closure of an RH4 valve cannot be defeated by any failure in the interlocking circuitry (i.e., an opening permissive from the SJ44 valve interlock would not cause automatic opening of RH4 nor would it prevent closure of RH4).

Valves 11SJ44 and 12SJ44

Unit 1 and 2 manual mode:

These are the containment sump valves which provide suction to the RHR pumps during the recirculation phase of a LOCA. The opening of each valve is enabled by the closure of its respective RH4 valve. The normal status of these valves is "closed" with control power "locked out" in the Control Room. Unit 2 control power "locked out" feature was removed to facilitate automatic opening of the sump valves upon receipt of a switchover sequence signal.

The purpose of the interlock is to assure that spurious opening of the valve will not result in emptying the RWST into the containment sump. The interlocks are fully independent on a "Train" basis so that failures could affect only one RHR pumping path. The required safety function of these valves is to open when initiating recirculation after the RH4 valves have been closed.

A failure of the interlock in a manner tending to prematurely open an SJ44 valve would have no consequence since a valve open position must be selected by an administratively controlled SJ44 hand switch. A failure of the interlock in a manner which prevents opening the sump valve is acceptable since the other pumping path would not be affected by this interlock failure.

Unit 2 semi-automatic mode:

When the semi-automatic mod is selected for Unit 2 the containment sump valve opens when a RWST low level occurs, bypassing the closure of the RH4 valve. The RH4 valves will remain open during opening of SJ44 ensuring RHR pump suction at all times. Once the SJ44 valve is fully open its respective RH4 valve automatically closes, fulfilling the interlock purpose of not emptying the RWST into the containment sump. The semi-automatic mode is fully independent on a "Train" basis so that failures could affect only one RHR pumping path.

The required safety function of these valves is to open when initiating recirculation and to provide closure permissive to the RH4 valves.

A failure of the interlock in a manner tending to prematurely open an SJ44 valve would have no consequence since two out of four RWST low level logic signals must also occur. A failure of the interlock in a manner which prevents opening the sump valve is acceptable since the other pumping path would not be affected by this interlock failure.

Valves 1SJ67 and 1SJ68

These are the safety injection pump miniflow line valves which allow flow back to the RWST. The valves are both normally open

with the control power "locked out" in the main Control Room to assure that the safety injection pumps have a flow path until RCS pressure falls below the shutoff head of the pumps. These valves are to be closed when transferring to the recirculation phase of a LOCA. The opening of either valve is enabled by the "closed" condition of valves 11SJ45 and 12SJ45. The closing of these valves is not interlocked.

A failure of the interlock circuitry tending to open the valve would have no consequence because the normal position of the valve is open, and it also has control power "locked out." The interlock circuitry could not fail in a manner which would automatically open the valve or prevent its closure. If the interlock were to fail subsequent to the valve's being closed for recirculation, only one of the valves could be affected by the failure. The valve affected in this case would not open unless the operator erroneously initiated an "open" signal from the main control console. Even if this were to occur, the redundant valve would remain closed.

Valves 11CS36 and 12CS36

These valves are opened in the recirculation phase of a LOCA to provide flow to the containment spray headers from the RHR system. The normal position of the valve is "closed" and opening requires the opening of its associated containment sump valve (11SJ44 interlocks 11CS36 and 12SJ44 interlocks 12CS36) and the closure of either 1RH1 or 1RH2 (the normal RHR cooldown path from the RCS). The devices used to develop the interlocks are redundant so that any interlock failure would affect only one of the CS36 valves.

Interlock failures tending to prevent opening of the valve can affect only one pumping path; the other path would provide the safety function. Interlock failures which would tend to open a valve prematurely are acceptable since such failures alone are not sufficient to open the valves (operator action is required in addition to fulfilling the interlock requirements).

Valves 11SJ45 and 12SJ45

These valves are used in independent piping loops during the recirculation phase of a LOCA to provide suction to the high head pumps from the RHR pumps. The required safety function of these valves is to open. Each valve's opening circuitry is enabled by the closure of either 1RH1 or IRH2, the opening of its associated sump valve (11SJ44 interlocks 11SJ45; 12SJ44 interlocks 12SJ45), and the closure of either ISJ67 or 1SJ68. The devices used to develop these interlocks are redundant such that any interlock failure affects only one valve.

Interlock failures tending to prevent opening of the valve can affect only one pumping path; the other path would provide the safety function. Interlock failures which would tend to open a valve prematurely are acceptable since such failures alone are not sufficient to open the valves (operator action is also required).

The circuits for valves 1SJ67 and 1SJ68 which provide the opening interlock for valves 11SJ45 and 12SJ45 have been moved to 125 V dc circuits not affected by containment flooding following a LOCA.

Valves 11SJ49 and 12SJ49

These valves are used to discharge RWST water from the RHR pumps to the Reactor Coolant System during the injection phase of a large break LOCA. In the injection phase these valves are not redundant and it is required that flow be injected into three of the four cold legs (one leg is assumed to dump to the floor). During the cold leg recirculation phase, the SJ49's are redundant, since only one valve is required to close to provide containment spray.

The control power lockout scheme was modified on these valves, as shown in Figure 7.3-4, due to voltage drop considerations during a LOCA with a degraded grid condition, which was not low enough to

separate the station from the offsite power source. These valves and the SJ54 valves were susceptible to this problem due to the large contractor size and the extended cable lengths. Since the SJ49 has the requirement for restoring power from the control room during an accident condition within approximately one hour of the accident starting time, the use of interposing relays has in the new circuit design resolved the problem in a degraded grid condition and the single failure criterion.

7.3.3 References for Section 7.3

1. Katz, D. N., "Solid State Logic Protection System Description," WCAP-7488-L (Proprietary), January 1971 and WCAP-7672 (Non-Proprietary), June 1971.

2. "Technical Manual - Control Electronics Unit (CEU) and Test Panel," Eaton document TM7N306 (PSBP #314197).