ATTACHMENT 1

TECHNICAL SPECIFICATION CHANGES

(MARKED-UP)

TABLE 3.3-3 (Continued)

ENGINEERED SAFETY FEATURES ACTUATION SYSTEM INSTRUMENTATION

FUNCTIONAL UNIT	TOTAL NO. OF CHANNELS	CHANNELS TO TRIP	MINIMUM CHANNELS OPERABLE	APPLICABLE MODES	ACTION
3. Containment Isolation (continued)					
2) Automatic Actuation Logic and Actuation Relays (SSPS)	2	1	2	1, 2, 3, 4	17
3) Automatic Actuation Logic and Actuation Relays (BOP ESFAS)	2	1	2	1, 2, 3, 4	17
4) Phase "A" Isolation	See Item 3.a. for all Phase "A" Isolation initiating functions and requirements.				
4. Steam Line Isolation					
a. Manual Initiation					
1) Individual	1/steam line	1/steam line	1/operating steam line	1, 2, 3	23
2) System	2	1	2	1, 2, 3	22
b. 1) Automatic Actuation Logic and Actuation Relays (SSPS)	2	1	2	1, 2, 3	34
c. Containment Pressure-High-2	3	2	2	1, 2, 3	33*
d. Steam Line Pressure-Low	3/steam line	2/steam line any steam line	2/steam line	1, 2, 3#	33*
e. Steam Line Pressure-Negative Rate-High	3/steam line	2/steam line any steam line	2/steam line	3##	33*
2) Automatic Actuation Logic and Actuation RELAYS (MSFIS)	3/SSPS Train	2/SSPS Train	2/SSPS Train	1,2,3	34a

CALLAWAY - UNIT 1

3/4 3-16

Amendment No. 89

TABLE 3.3-3 (Continued)

ENGINEERED SAFETY FEATURES ACTUATION SYSTEM INSTRUMENTATION

FUNCTIONAL UNIT	TOTAL NO. OF CHANNELS	CHANNELS TO TRIP	MINIMUM CHANNELS OPERABLE	APPLICABLE MODES	ACTION
5. Feedwater Isolation & Turbine Trip					
a. 1) Automatic Actuation Logic and Actuation Relays (SSPS)	2	1	2	1, 2	27
b. Steam Generator Water Level High-High	4/stm. gen.	2/stm. gen. in any operating stm. gen.	3/stm. gen. in each operating stm. gen.	1, 2	33*
c. Safety Injection	See Item 1. above for all Safety Injection initiating functions and requirements.				
6. Auxiliary Feedwater					
a. Manual Initiation	3(1/pump)	1/pump	1/pump	1, 2, 3	24
b. Automatic Actuation Logic and Actuation Relays (SSPS)	2	1	2	1, 2, 3	34
c. Automatic Actuation Logic and Actuation Relays (BOP ESFAS)	2	1	2	1, 2, 3	21
d. Steam Generator Water Level Low-Low					
1) Start Motor-Driven Pumps					
a) Steam Generator Water Level Low-Low (Adverse Containment Environment)	4/stm. gen.	2/stm. gen. in any operating stm. gen.	3/stm. gen. in each operating stm. gen.	1, 2, 3	33*, 35
a. 2) Automatic Actuation Logic and Actuation Relays (MSPSS)	3/SSPS Train	2/SSPS Train	2/SSPS train	1,2	27a

TSI 33

TABLE 3.3-3 (continued)
ACTION STATEMENTS (continued)

ACTION 25 - With the number of OPERABLE channels one less than the Minimum Channels OPERABLE requirement, declare the affected diesel generator and off-site power source inoperable and take the ACTION required by Specification 3.8.1.1 or 3.8.1.2.

ACTION 26 - With the number of OPERABLE channels one less than the Minimum Channels OPERABLE requirement, restore the inoperable channel to OPERABLE status within 48 hours or initiate and maintain operation of the Control Room Emergency Ventilation System.

ACTION 27 - With the number of OPERABLE channels one less than the Minimum Channels OPERABLE requirement, be in at least HOT STANDBY within 12 hours; however, one channel may be bypassed for up to 4 hours for surveillance testing per Specification 4.3.2.1 provided the other channel is OPERABLE.

INSERT 1 →

(NOTE: ACTION STATEMENTS 28 THROUGH 31 ARE LOCATED ON OTHER TABLES.)

TSI 62

TSI 33

TABLE 3.3-3 (Continued)

ACTION STATEMENTS (Continued)

ACTION 32 - With the number of OPERABLE channels one less than the Total Number of Channels, except for testing, STARTUP and/or POWER OPERATION may proceed for up to 72 hours provided the following conditions are satisfied:

a. The inoperable channel is placed in the tripped condition within 6 hours, and

b. The Minimum Channels OPERABLE requirement is met; however, the inoperable channel may be bypassed for up to 4 hours for surveillance testing of other channels per Specification 4.3.2.1.

Restore the inoperable channel to OPERABLE status within 72 hours or be in at least HOT STANDBY within the next 6 hours and in COLD SHUTDOWN within the following 30 hours.

With the number of OPERABLE channels one less than the Total Number of Channels due to testing of a channel, that channel may be tripped for up to 4 hours for surveillance testing per Specification 4.3.2.1.

ACTION 33 - With the number of OPERABLE channels one less than the Total Number of Channels, STARTUP and/or POWER OPERATION may proceed provided the following conditions are satisfied:

a. The inoperable channel is placed in the tripped condition within 6 hours, and

b. The Minimum Channels OPERABLE requirement is met; however, the inoperable channel may be bypassed for up to 4 hours for surveillance testing of other channels per Specification 4.3.2.1.

ACTION 34 - With the number of OPERABLE channels one less than the Minimum Channels OPERABLE requirement, be in at least HOT STANDBY within 12 hours and in at least HOT SHUTDOWN within the following 6 hours; however, one channel may be bypassed for up to 4 hours for surveillance testing per Specification 4.3.2.1 provided the other channel is OPERABLE.

INSERT 2 →

ACTION 35 - With an inoperable delay timer in the Trip Time Delay circuitry, STARTUP and/or POWER OPERATION may proceed provided that the Vessel ΔT (Power-1, Power-2) channels in the affected protection sets are placed in the tripped condition within 6 hours.

INSERTS TO TABLE 3.3-3

INSERT 1

ACTION 27a - With the number of OPERABLE channels one less than the Total Number of Channels, operation may proceed. The inoperable channel fails to a non-tripped condition. With the number of OPERABLE channels one less than the Minimum Channels OPERABLE requirement, be in at least HOT STANDBY within 12 hours. One train may be placed in test for up to 4 hours for surveillance testing per Specification 4.3.2.1 provided the other train is OPERABLE.

INSERT 2

ACTION 34a - With the number of OPERABLE channels one less than the Total Number of Channels, operation may proceed. The inoperable channel fails to a non-tripped condition. With the number of OPERABLE channels one less than the Minimum Channels OPERABLE requirement, be in at least HOT STANDBY within 12 hours and in at least HOT SHUTDOWN within the following 6 hours. One train may be placed in test for up to 4 hours for surveillance testing per Specification 4.3.2.1 provided the other train is OPERABLE.

TABLE 3.3-4 (Continued)

ENGINEERED SAFETY FEATURES ACTUATION SYSTEM INSTRUMENTATION TRIP SETPOINTS

FUNCTIONAL UNIT	TOTAL ALLOWANCE (TA)	Z	SENSOR ERROR (S)	TRIP SETPOINT	ALLOWABLE VALUE
3. Containment Isolation (Continued)					
3) Automatic Actuation Logic and Actuation Relays (BOP ESFAS)	N.A.	N.A.	N.A.	N.A.	N.A.
4) Phase "A" Isolation	See Item 3.a. above for all Phase "A" Isolation Trip Setpoints and Allowable Values.				
4. Steam Line Isolation					
a. Manual Initiation	N.A.	N.A.	N.A.	N.A.	N.A.
b.1) Automatic Actuation Logic and Actuation Relays (SSPS)	N.A.	N.A.	N.A.	N.A.	N.A.
b.2) c. Containment Pressure-High-2	4.3	0.71	2.0	$\leq$ 17.0 psig	$\leq$ 18.3 psig
d. Steam Line Pressure-Low	19.6	14.81	2.0	$\geq$ 615 psig	$\geq$ 571 psig*
e. Steam Line Pressure Negative Rate - High	3.0	0.5	0	$\leq$ 100 psi	$\leq$ 124 psi**
5. Feedwater Isolation & Turbine Trip					
a.1) Automatic Actuation Logic and Actuation Relays (SSPS)	N.A.	N.A	N.A.	N.A.	N.A.
a.2) Automatic Actuation Logic and Actuation Relays (MSFIS)	N.A.	N.A.	N.A.	N.A.	N.A.

TABLE 4.3-2 (Continued)

ENGINEERED SAFETY FEATURES ACTUATION SYSTEM INSTRUMENTATION

SURVEILLANCE REQUIREMENTS

FUNCTIONAL UNIT	CHANNEL CHECK	CHANNEL CALIBRATION	ANALOG CHANNEL OPERATIONAL TEST	TRIP ACTUATING DEVICE OPERATIONAL TEST	ACTUATION LOGIC TEST	MASTER RELAY TEST	SLAVE RELAY TEST	MODES FOR WHICH SURVEILLANCE IS REQUIRED
4. Steam Line Isolation								
a. Manual Initiation	N.A.	N.A.	N.A.	R	N.A.	N.A.	N.A.	1, 2, 3
b.1) Automatic Actuation Logic and Actuation Relays (SSPS)	N.A.	N.A.	N.A.	N.A.	M(1)	M(1)	Q	1, 2, 3
INSERT 3 → c. Containment Pressure-High-2	S	R	Q	N.A.	N.A.	N.A.	N.A.	1, 2, 3
d. Steam Line Pressure-Low	S	R	Q	N.A.	N.A.	N.A.	N.A.	1, 2, 3
e. Steam Line Pressure-Negative Rate-High	S	R	Q	N.A.	N.A.	N.A.	N.A.	3
5. Feedwater Isolation & Turbine Trip								
a.1) Automatic Actuation Logic and Actuation Relays (SSPS)	N.A.	N.A.	N.A.	N.A.	M(1)	M(1)	Q(3)	1, 2
INSERT 4 → b. Steam Generator Water Level-High-High	S	R	Q	N.A.	N.A.	N.A.	N.A.	1, 2
c. Safety Injection	See Item 1. above for all Safety Injection Surveillance Requ							
6. Auxiliary Feedwater								
a. Manual Initiation	N.A.	N.A.	N.A.	R	N.A.	N.A.	N.A.	1, 2, 3
b Automatic Actuation Logic and Actuation Relays (SSPS)	N.A.	N.A.	N.A.	N.A.	M(1)	M(1)	Q	1, 2, 3

INSERTS TO TABLE 4.3-2

INSERT 3

b.2)	Automatic Actuation Logic and Actuation Relays (MSFIS)	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	Q	1,2,3

INSERT 4

a.2)	Automatic Actuation Logic and Actuation Relays (MSFIS)	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	Q(3)	1,2

ATTACHMENT 2

TECHNICAL SPECIFICATION CHANGES

(RE-TYPED)

TABLE 3.3-3 (Continued)

ENGINEERED SAFETY FEATURES ACTUATION SYSTEM INSTRUMENTATION

FUNCTIONAL UNIT	TOTAL NO. OF CHANNELS	CHANNELS TO TRIP	MINIMUM CHANNELS OPERABLE	APPLICABLE MODES	ACTION
3. Containment Isolation (continued)					
2) Automatic Actuation Logic and Actuation Relays (SSPS)	2	1	2	1, 2, 3, 4	17
3) Automatic Actuation Logic and Actuation Logic and Actuation Relays (BOP ESFAS)	2	1	2	1, 2, 3, 4	17
4) Phase "A" Isolation	See Item 3.a. for all Phase "A" Isolation initiating functions and requirements.				
4. Steam Line Isolation					
a. Manual Initiation					
1) Individual	1/steam line	1/steam line	1/operating steam line	1, 2, 3	23
2) System	2	1	2	1, 2, 3	22
b. 1) Automatic Actuation Logic and Actuation Relays (SSPS)	2	1	2	1, 2, 3	34
2) Automatic Actuation Logic and Actuation Relays (MSFIS)	3/SSPS Train	2/SSPS Train	2/SSPS Train	1, 2, 3	34a
c. Containment Pressure-High-2	3	2	2	1, 2, 3	33*
d. Steam Line Pressure-Low	3/steam line	2/steam line and steam line	2/steam line	1, 2, 3#	33*
e. Steam Line Pressure-Negative Rate-High	3/steam line	2/steam line any steam line	2/steam line	3##	33*

TABLE 3.3-3 (Continued)

ENGINEERED SAFETY FEATURES ACTUATION SYSTEM INSTRUMENTATION

FUNCTIONAL UNIT	TOTAL NO. OF CHANNELS	CHANNELS TO TRIP	MINIMUM CHANNELS OPERABLE	APPLICABLE MODES	ACTION
5. Feedwater Isolation & Turbine Trip					
a. 1) Automatic Actuation Logic and Actuation Relays (SSPS)	2	1	2	1, 2	27
2) Automatic Actuation Logic and Actuation Relays (MSFIS)	3/SSPS Train	2/SSPS Train	2/SSPS Train	1,2	27a
b. Steam Generator Water Level High-High	4/stm. gen.	2/stm. gen. in any operating stm. gen.	3/stm. gen. in each operating stm. gen.	1, 2	33*
c. Safety Injection	See Item 1. above for all Safety Injection initiating functions and requirements.				
6. Auxiliary Feedwater					
a. Manual Initiation	3(1/pump)	1/pump	1/pump	1,2, 3	24
b. Automatic Actuation Logic and Actuation Relays (SSPS)	2	1	2	1, 2, 3	34
c. Automatic Actuation Logic and Actuation Relays (BOP ESFAS)	2	1	2	1, 2, 3	21
d. Steam Generator Water Level Low-Low					
1) Start Motor-Driven Pumps					
a) Steam Generator Water Level Low-Low (Adverse Containment Environment)	4/stm. gen.	2/stm. gen. in any operating stm. gen.	3/stm. gen. in each operating stm. gen.	1, 2, 3	33*, 35

ACTION 25 - With the number of OPERABLE channels one less than the Minimum Channels OPERABLE requirement, declare the affected diesel generator and off-site power source inoperable and take the ACTION required by Specification 3.8.1.1 or 3.8.1.2.

ACTION 26 - With the number of OPERABLE channels one less than the Minimum Channels OPERABLE requirement, restore the inoperable channel to OPERABLE status within 48 hours or initiate and maintain operation of the Control Room Emergency Ventilation System.

ACTION 27 - With the number of OPERABLE channels one less than the Minimum Channels OPERABLE requirement, be in at lest HOT STANDBY within 12 hours; however, one channel may be bypassed for up to 4 hours for surveillance testing per Specification 4.3.2.1 provided the other channel is OPERABLE.

ACTION 27a - With the number of OPERABLE channels one less than the Total Number of Channels, operation may proceed. The inoperable channel fails to a non-tripped condition. With the number of OPERABLE channels one less than the Minimum Channels OPERABLE requirement, be in at least HOT STANDBY within 12 hours. One train may be placed in test for up to 4 hours for surveillance testing per Specification 4.3.2.1 provided the other train is OPERABLE.

(NOTE: ACTION STATEMENTS 28 THROUGH 31 ARE LOCATED ON OTHER TABLES.)

ACTION 32 - With the number of OPERABLE channels one less than the Total Number of Channels, except for testing, STARTUP and/or POWER OPERATION may proceed for up to 72 hours provided the following conditions are satisfied:

a. The inoperable channel is placed in the tripped condition within 6 hours, and

b. The Minimum Channels OPERABLE requirement is met; however, the inoperable channel may be bypassed for up to 4 hours for surveillance testing of other channels per Specification 4.3.2.1.

Restore the inoperable channel to OPERABLE status within 72 hours or be in at least HOT STANDBY within the next 6 hours and in COLD SHUTDOWN within the following 30 hours.

With the number of OPERABLE channels one less than the Total Number of Channels due to testing of a channel, that channel may be tripped for up to 4 hours for surveillance testing per Specification 4.3.2.1.

ACTION 33 - With the number of OPERABLE channels one less than the Total Number of Channels, STARTUP and/or POWER OPERATION may proceed provided the following conditions are satisfied:

a. The inoperable channel is placed in the tripped condition within 6 hours, and

b. The Minimum Channels OPERABLE requirement is met; however, the inoperable channel may be bypassed for up to 4 hours for surveillance testing of other channels per Specification 4.3.2.1.

ACTION 34 - With the number of OPERABLE channels one less than the Minimum Channels OPERABLE requirement, be in at least HOT STANDBY within 12 hours and in at leat HOT SHUTDOWN within the following 6 hours; however, one channel may be bypassed for up to 4 hours for surveillance testing per Specification 4.3.2.1 provided the other channel is OPERABLE.

ACTION 34a - With the number of OPERABLE channels one less than the Total Number of Channels, operation may proceed. The inoperable channel fails to a non-tripped condition. With the number of OPERABLE channels one less than the Minimum Channels OPERABLE requirement, be in at least HOT STANDBY within 12 hours and in at least HOT SHUTDOWN within the following 6 hours. One train may be placed in test for up to 4 hours for surveillance testing per Specification 4.3.2.1 provided the other train is OPERABLE.

ACTION 35 - With an inoperable delay timer in the Trip Time Delay circuitry, STARTUP and/or POWER OPERATION may proceed provided that the Vessel ΔT (Power-1, Power-2) channels in the affected protection sets are placed in the tripped condition within 6 hours.

ENGINEERED SAFETY FEATURES ACTUATION SYSTEM INSTRUMENTATION TRIP SETPOINTS

FUNCTIONAL UNIT	TOTAL ALLOWANCE (TA)	Z	SENSOR ERROR (S)	TRIP SETPOINT	ALLOWABLE VALUE
3. Containment Isolation (Continued)					
3) Automatic Actuation Logic and Actuation Relays (BOP ESFAS)	N.A.	N.A.	N.A.	N.A.	N.A.
4) Phase "A" Isolation	See Item 3.a. above for all Phase "A" Isolation Trip Setpoints and Allowable Values.				
4. Steam Line Isolation					
a. Manual Initiation	N.A.	N.A.	N.A.	N.A.	N.A.
b. 1) Automatic Actuation Logic and Actuation Relays (SSPS)	N.A.	N.A.	N.A.	N.A.	N.A.
2) Automatic Actuation Logic and Actuation Relays (MSFIS)	N.A.	N.A.	N.A.	N.A.	N.A.
c. Containment Pressure-High-2	4.3	0.71	2.0	$\leq$ 17.0 psig	$\leq$ 18.3 psig
d. Steam Line Pressure-Low	19.6	14.81	2.0	$\geq$ 615 psig	$\geq$ 571 psig*
e. Steam Line Pressure Negative Rate - High	3.0	0.5	0	$\leq$ 100 psi	$\leq$ 124 psi**
5. Feedwater Isolation & Turbine Trip					
a. 1) Automatic Actuation Logic and Actuation Relays (SSPS)	N.A.	N.A.	N.A.	N.A.	N.A.
2) Automatic Actuation Logic and Actuation Relays (MSFIS)	N.A.	N.A.	N.A.	N.A.	N.A.

TABLE 4.3-2 (Continued)

ENGINEERED SAFETY FEATURES ACTUATION SYSTEM INSTRUMENTATION
SURVEILLANCE REQUIREMENTS

FUNCTIONAL UNIT	CHANNEL CHECK	CHANNEL CALIBRATION	ANALOG CHANNEL OPERATIONAL TEST	TRIP ACTUATING DEVICE OPERATIONAL TEST	ACTUATION LOGIC TEST	MASTER RELAY TEST	SLAVE RELAY TEST	MODES FOR WHICH SURVEILLANCE IS REQUIRED
4. Steam Line Isolation								
a. Manual Initiation	N.A.	N.A.	N.A.	R	N.A.	N.A.	N.A.	1, 2, 3
b.1. Automatic Actuation Logic and Actuation Relays (SSPS)	N.A	N.A.	N.A.	N.A.	M(1)	M(1)	Q	1, 2, 3
b.2. Automatic Actuation Logic and Actuation Relays (MSFIS)	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	Q	1, 2, 3
c. Containment Pressure-High-2	S	R	Q	N.A.	N.A.	N.A.	N.A.	1, 2, 3
d. Steam Line Pressure-Low	S	R	Q	N.A.	N.A.	N.A.	N.A.	1, 2, 3
e. Steam Line Pressure-Negative Rate-High	S	R	Q	N.A.	N.A.	N.A.	N.A.	3
5. Feedwater Isolation & Turbine Trip								
a.1. Automatic Actuation Logic and Actuation Relays (SSPS)	N.A.	N.A.	N.A.	N.A.	M(1)	M(1)	Q(3)	1, 2
a.2. Automatic Actuation Logic and Actuation Relays (MSFIS)	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	Q(3)	1, 2
b. Steam Generator Water Level-High-High	S	R	Q	N.A.	N.A.	N.A.	N.A.	1, 2
c. Safety Injection	See Item 1 above for all Safety Injection Surveillance Requirements.							
6. Auxiliary Feedwater								
a. Manual Initiation	N.A.	N.A.	N.A.	R	N.A.	N.A.	N.A.	1, 2, 3
b. Automatic Actuation Logic and Actuation Relays (SSPS)	N.A.	N.A.	N.A.	N.A.	M(1)	M(1)	Q	1, 2, 3

ATTACHMENT 3

SAFETY EVALUATION

Executive Summary		Page 1
Glossary of Terms		Page 2
Section 1:	Background of the Current MSFIS System	Page 3
Section 2:	Description of the MSFIS Modification	Page 4
Section 3:	Formal Safety Evaluation	Page 14

SAFETY EVALUATION FOR THE CALLAWAY PLANT MSFIS MODIFICATION AND TECHNICAL SPECIFICATION AMENDMENT

EXECUTIVE SUMMARY

This license amendment requests a revision to Technical Specification (TS) 3/4.3.2 "Engineered Safety Features Actuation System Instrumentation." This specification is revised by adding the Main Steam and Feedwater Isolation System (MSFIS) actuation logic and relays to Functional Units 4.b and 5.a of Tables 3.3-3, 3.3-4, and 4.3-2. Table 3.3-3 is further revised by the addition of Action Statements 27a and 34a, which provide guidance in the event of an inoperable MSFIS channel or train. These proposed changes are the result of a modification that will replace existing digital portions of the MSFIS with digital processor equipment.

The existing MSFIS logic is considered part of the Solid State Protection System (SSPS) in TS. Currently, if one train of MSFIS is inoperable, then one train of SSPS is inoperable. The modified MSFIS will have a two out of three logic channel design for each train. The addition of MSFIS actuation logic and relays to TS Tables 3.3-3, 3.3-4, and 4.3-2 allows one channel of MSFIS to be declared inoperable or placed in test without declaring the corresponding train of SSPS inoperable.

Based upon discussions with the NRC Staff and the review criteria provided in NRC Generic Letter 95-02, "Use of NUMARC/EPRI Report TR-102348, 'Guideline on Licensing Digital Upgrades,' in Determining the Acceptability of Performing Analog-to-Digital Replacements Under 10 CFR 50.59," this application requires NRC approval because the following three areas of the MSFIS modification involve an unreviewed safety question:

(1) The MSFIS design will use software which could result in a common mode failure;

(2) The original NRC review of the MSFIS did not evaluate 2 out of 3 coincidence circuitry, which could introduce new system failure modes; and,

(3) The MSFIS modification utilizes manual handswitches that could introduce new system failure modes.

These failure modes and the unreviewed safety question are discussed further in this safety evaluation. Union Electric has determined that the MSFIS modification and proposed Technical Specification change will not adversely affect the health and safety of the public.

Glossary of Terms

A-B	Allen Bradley
AC	Alternating Current
EMI	Electromagnetic Interference
EPROM	Erasable Programmable Read Only Memory
ESFAS	Engineered Safety Feature Actuation System
ESD	Electrostatic Discharge
ESF	Engineered Safety Feature
FAT	Factory Acceptance Test
FIV	Feedwater Isolation Valve
FSAR	Final Safety Analysis Report
FWIS	Feedwater Isolation Signal
HEX	Binary Computer Code
HDD	Hardware Design Documents
HRS	Hardware Requirements Specification
ICOM	Software Developer
LLD	Ladder Logic Diagrams
MCB	Main Control Board
MFCV	Main Feedwater Control Valve
MSFIS	Main Steam and Feedwater Isolation System
MSIV	Main Steam Isolation Valve
MTBF	Mean Time Before Failure
NTS	Nuclear Testing Systems
PC	Personal Computer
PLC	Programmable Logic Controller
PROM	Programmable Read Only Memory
RFI	Radio Frequency Interference
RPS	Reactor Protection System
SAT	Site Acceptance Test
SBLOCA	Small Break Loss of Coolant Accident
SDD	Software Design Documents
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SHAT	Software/Hardware Acceptance Test
SNCR	Software Nonconformance Report
SP	Spectrum Technologies, USA, Inc.
SRD	System Requirements Document
SRS	Software Requirements Specification
SSPS	Solid State Protection System
SUT	Software Unit Test
SUTR	Software Unit Test Report
VDC	Volts Direct Current
V&V	Verification and Validation
WDT	Watchdog Timer
WVR	Walkthrough Verification Report

SECTION 1: BACKGROUND OF THE CURRENT MSFIS SYSTEM

The Main Steam and Feedwater Isolation System (MSFIS) consists of two independent actuation trains. Each of the actuation trains monitors system inputs and by means of logic matrices, drive actuation relays that energize or deenergize the solenoids required for the appropriate Main Steam Isolation Valve (MSIV) or Feedwater Isolation Valve (FIV) operation. Each MSIV or FIV has redundant hydraulic actuators, one side Active and the other Standby. Both actuators operate the same, except they have different control signals. The Active sides have Fast Close (FC), Slow Open, Slow Close, 10% Close, Exercise, Engineered Safety Feature Actuation System (ESFAS) and Accumulator Pre-Charge for control signals. The Standby sides do not have Slow Open and Slow Close sequences. The current control logic circuitry is of a single logic solid state design (see Figure 1), except for the electromechanical relays used as the final output devices.

The MSFIS accepts input signals for the MSIV/FIVs in the form of contact conditions from the Main Control Board (MCB) switches (such as 10% close exercise, Slow Open, Slow Close, Accumulator Test, and Manual Fast Close), MSFIS Test Panel rotary switches, the ESFAS output relays and from MSIV or FIV position limit switches. The input signals are processed through an input buffer for isolation, into a valve control logic card that provides the necessary timing intervals for valve operations, and to an output relay driver to energize or de-energize the actuation relays and solenoids for each valve. The MSFIS Test Panel is used to verify proper operation of the selected valve control logic circuitry and the fast close signal from the input buffer through to the relay output driver. The operation of an eight position switch for each valve provides the testing functions. The first clockwise position from "Operate" is "Bypass", which will prevent inadvertent actuation of any valve prior to any testing.

MSFIS processes the safety inputs from ESFAS and Manual Fast Close to produce the desired safety signals. However, failures have occurred on the printed circuit boards that produce actuation signals that close either an MSIV or FIV. Closure of either valve at power has caused plant trips and reduced plant availability.

Final Safety Analysis Report (FSAR) Sections 7.3.7 and 7.3.8 state that the MSFIS provides control to the MSIV and FIV actuators from separate Class IE electrical systems capable of closing each valve independently of the other. The MSIVs are part of the Main Steam Supply System and isolate the non-safety

portion of the system (FSAR Section 10.3). The FIVs are installed to prevent an uncontrolled blowdown from more than one Steam Generator in the event of a feedwater pipe rupture in the Turbine Building and isolate the non-safety portions of the Feedwater system (FSAR Section 10.4.7).

SECTION 2: DESCRIPTION OF THE MSFIS MODIFICATION

The MSFIS was identified as a single point failure system that could cause plant trips. As a result, UE developed Specification J-1065 for the MSFIS replacement. This specification was sent out to several safety-related Appendix B suppliers. Spectrum Technologies, USA, Inc. (SP) was selected as the vendor to supply the new equipment. Throughout the design process, UE interfaced with SP to ensure the plant specific design requirements were met. UE participated in a conceptual design review and interim design review, and will participate in a Factory Acceptance Test at SP. SP visited Callaway Plant to walkdown specific details associated with the design. Various comments and discrepancies were generated by UE and SP throughout the design and testing with subsequent resolution by both parties, as required.

The MSFIS replacement was designed and developed by SP utilizing Allen Bradley (A-B) Programmable Logic Controllers (PLCs) which perform the same logic as the current system design. The A-B PLCs are a 5/25 type that use A-B PLC firmware of the PLC-5 family of controllers and ICOM ladder logic software to develop the application software. SP is a 10CFR50 Appendix B supplier and is on UE's Quality Supplier List. SP purchased the MSFIS equipment and provided commercial grade dedication for its safety related functions. SP has been successfully audited by NUPIC, and in November 1995, UE and Data Refining Technologies performed a critical design review of the MSFIS design at SP and found no significant concerns. Since the current digital logic will be replaced with a PLC that is controlled by a digital processor, this modification is a digital to digital conversion.

The system is composed of triple redundant logic consisting of three logic channels in two different trains or separation groups. The triple redundant logic will provide the MSFIS equipment with a 2 out of 3 voting scheme (see Figure 2). The output module contacts for each logic channel are normally open and close to trip. The 2 out of 3 voting scheme solves the problem of a 1 out of 2 nuisance actuation. To trigger an actuation, two logic channels (i.e., A-B, A-C, or B-C) per train trip and energize the actuation relays. Each train of MSFIS contains 3 PLCs, one for each logic channel. This logic design requires coincidence testing to ensure each set of combinations can produce an actuation. The 2 out of 3 logic design increases

plant reliability and availability. A single failure cannot trigger a false actuation, nor prevent a true actuation from occurring. If one logic channel fails, the affected train reverts to a 2 out of 2 logic. If a PLC channel failure occurs, a Channel Failure light will energize on the MSFIS test panel and the MCB annunciation of the Channel Failure will occur. This is discussed further in Section 3 of this evaluation. UE performed a Probability Risk Assessment that evaluated this logic scheme. This assessment showed that decreased risk of spurious actuation results in decreased risk of transient induced trips plant trips.

The Solid State Protection System (SSPS) and Reactor Protection System (RPS) input the ESFAS signals, and the MCB hand switches input to the MSFIS cabinets, SA075A and SA075B. The existing actuation output relays, input terminal boards, and output terminal boards are used. The man-machine interface for operators and maintenance technicians is similar to the existing configuration, except that local PLC fault indication and coincidence logic test functions are provided. The coincidence logic test functions are performed on the MSFIS test panel where each combination of input signals can be tested.

Each MSFIS cabinet consists of three A-B 5/25 PLCs, external watchdog timers, interposing (actuation) relays, a 125/48 VDC converter to provide voltage to energize the actuation relays and energizing voltage for input signal contacts, and a test panel. The test panel contains indicators and controls to perform the following functions: place each valve into Test or Operate mode, exercise one or more valves through a pre-defined sequence, simulate inputs to each valve, indicate test mode for each valve, control DC power to and reset each logic channel, indicate channel failure for each logic channel, and perform coincidence testing of the three logic channels. The PLC contains input modules that read the input signals, a digital processor to implement the logic, output modules to control the output devices (actuation relays and status indicators), and a 125/5 VDC power supply to operate the PLC.

Each MSFIS cabinet contains toggle switches, located on the Emergency Override Panel, for each of the four MSIVs and four FIVs. With a Feedwater Isolation Signal present, the FIV toggle switches (NORMAL and BYPASS positions) provide a bypass to the Feedwater Isolation Signal to allow opening of the FIVs to supply feed flow to the Steam Generators. This bypass annunciates on the ESF Status Panels for each FIV. The toggle switches (NORMAL and FC positions) for the MSIVs are used to provide a diverse means to manually fast close the MSIVs in the event of a common mode software failure coincident with an accident requiring an MSIV closure.

Software

The software is designed in accordance with ANSI/IEEE-ANS-7-4.3.2-1993, "Criteria for Programmable Digital Computer System Software in Safety-Related Systems of Nuclear Power Plants," and ANSI/IEEE 1012-1986, "IEEE Standard for Software Verification and Validation Plans."

The application software was developed by SP utilizing A-B PLCs and ICOM programming software. Using structured design principles, the top level design of the MSFIS software is intended to be simple and straight forward. Interrupts (an event that would interrupt the normal program flowpath) is not used in the MSFIS software and all programs are single task (i.e., no multi-tasking - a program structure that performs multiple tasks simultaneously). The software is designed with a modular structure that is beneficial for testing and verification.

The software is developed and organized to consist of several software programs: Main, Initialize, Run, Input, Valve Logic, Output, Self Test, and Fault. The main program calls the Initialize and Run programs upon powerup of MSFIS. The initialize program resets all the timers, set system outputs to 0, and have the self test program check for minor faults before processing begins. The Run program "reads" the inputs, executes the valve logic, and "writes" to the outputs. If any program generates a fault, the Fault program generates the "Chan Fail" light. All application software resides in Erasable Programmable Read Only Memory (EPROM).

Verification is performed by SP personnel who are independent of the design processes. The SP Project Manager develops the source code or ladder logic and submits it to the V&V group for the code verification walkthroughs. Implementation of the Software Verification and Validation (V&V) Plan is the responsibility of the SP Quality Assurance group, which is independent of the project development group and reports directly to SP's President. The V&V Engineer performs and/or directs the performance of the V&V activities for the project. The Walkthrough Verification Report documents this review.

The V&V of the MSFIS replacement is a structured method that includes the SP V&V Plan, the review process and policies for technical reviews, software and hardware testing of normal and abnormal events, and an independent stage-to-stage verification of each phase of the software life cycle. SP's software life cycle follows the "waterfall model" (see Figure 3).

The V&V of the MSFIS hardware and software starts with UE Specification J-1065 and diverges to follow two paths until integration testing occurs at the end of the process. Initially, a System Requirement Document (SRD) was written and reviewed with UE to ensure all the requirements of J-1065 were met. Additional details of the software requirements and input/output requirements were specified in the Software and Hardware Requirements Specifications (SRS & HRS). Next, the specific subroutines and parameters were defined and hardware drawings were completed with the development of the Software and Hardware Design Documents (SDD & HDD). At this point, a joint review by UE and SP provided a line-by-line verification of requirements.

After the software was coded into the ladder logic diagrams (LLDs), the code was tested by a walk-through phase to verify compliance with the Software Design Document (SDD). The walkthrough verification provided a line-by-line review of the code to ensure the requirements of the SDD were correctly implemented, and that no unintended functions were present. Software Nonconformance Reports (SNCRs - traceability, software, and comments) were generated to document and resolve any errors that are reported in the Walkthrough Verification Report (WVR).

The software is then Module tested with Software Unit Tests (SUTs). Modules are well-defined software units that are independently testable with a predictable behavior. The SUTs test each module under all possible combinations of inputs and system parameters. Test procedures are developed for each module and the test results are documented in the Software Unit Test Report (SUTR). Once the SUTs are performed and verified, the Software/Hardware Acceptance Test (SHAT) validates that all individual modules can communicate correctly and verifies the integration of the hardware and software. Before the application software is loaded on the PLC, a Ladder Logic Report (the conversion of the binary ladder logic data file to a human readable text format) is generated. The application software is downloaded into the PLC 5/25 processor as a binary file. Also, the Programmable Read Only Memory (PROM) contents can be stored in HEX code prior to loading the EPROM, which can be compared bit-by-bit after loading.

The SHAT will be performed on a pre-production unit that is driven by a PC to emulate system inputs. The unit will be loaded with the application software and tested to verify functions specified in the design documents. Finally, the application software will be loaded onto the production units and tested with the hardware during a Factory Acceptance Test (FAT). The production units will be shipped to Callaway Plant and installed by site personnel. Following installation, the system will

undergo a Site Acceptance Test (SAT), which will be performed to verify and validate proper operation and complete surveillance procedures.

The application software is supplied in EPROM. The software code and documentation are kept under configuration management control by SP. A design modification will be required to make software changes after a review to determine the impact of the change on other components and the need for re-testing or modification of test procedures. All modified code will be subjected to the Verification and Validation process as described above.

Equipment Qualification

The MSFIS is designed to withstand the effects of natural phenomenon and is qualified to operate in normal and post accident conditions. The system is qualified to perform its intended safety function under the environmental conditions of temperature, humidity, seismic, electromagnetic and radio frequency interference (EMI & RFI), and radiation.

SP reviewed the specifications for the A-B equipment (and other provided equipment) for compliance with IEEE 323-1974, "IEEE Standard for Qualifying Class IE Equipment for Nuclear Power Generating Stations." The current MSFIS equipment is located in a mild environment and is designed to operate at a temperature of 60 to 120°F in a relative humidity of 30% to 70% without loss of protective function. The A-B equipment (and other provided equipment) is specified to operate at a temperature of 0 to 140°F in a relative humidity range of 5% to 95%. In addition, the MSFIS equipment is qualified to 1000 rads. Therefore, the new equipment is qualified for an environment that exceeds the existing design requirements.

The heat load of the new equipment is less than the existing equipment and will not challenge the cabinet or room temperature profiles.

The MSFIS cabinets will remain in place and utilize the existing terminal boards and actuation relays. Only the electronic circuit cards, card frames, power supplies and test panel will be removed. The MSFIS components will be subjected to multi-axis/frequency inputs in accordance with IEEE 344-1975, "IEEE Recommended Practices for Seismic Qualification of Class IE Equipment for Nuclear Power Generating Stations" to the SNUPPS seismic spectra profile. The components will be seismically tested with the application software running. The existing cabinets were previously qualified prior to installation and

seismic analysis will demonstrate the qualification of the new equipment installed in the existing cabinets.

SP will qualify the MSFIS replacement equipment in accordance with EPRI document, TR-102323-EMI guideline (IEC - International Standard 801 Parts 2-6 and MIL-STD-461 EMI Susceptibility and Emission Requirements) to meet the EPRI EMI limiting practices. The emission levels established for the Callaway Plant are enveloped by the testing performed by EPRI. The emission levels are established in the EPRI guide per the emission envelopes of CE (Conducted Emission) 102 and RE (Radiated Emission) 102. The susceptibility levels are established in the EPRI guide per IEC 801-4 (Fast Transients), IEC 801-5 (Surge Tests), CS (Conducted Susceptibility) 101 - Low Frequency, CS 114 - Hi Frequency, RS (Radiated Susceptibility) 103 - Electric Fields, and IEC 801-2 (Electrostatic Discharge). The components will be EMI/RFI tested at National Testing Services in Acton, Massachusetts.

The cabinets are located in the back of the Main Control Room next to other electronic instrumentation panels. The surrounding rooms are the upper and lower cable spreading rooms. Use of radio transceivers is prohibited in this area. This restriction limits high frequency radiated emission concerns. Any low frequency emission are attenuated by the small wavelength the cabinet openings present to low frequency signals that require a rather large wavelength in order to propagate.

Electrostatic discharge (ESD) can cause damage to electronic devices and has been known to cause lock-ups on digital equipment if a large enough discharge exists. Maintenance on the MSFIS requires prior installation of ESD grounding straps.

Interaction Between IE and Non-IE Equipment

The only interaction between the MSFIS and non-IE equipment is the connection to the plant annunciator system. These outputs are isolated by use of existing optical isolation devices located in the Plant Annunciator Isolator Cabinet installed as part of the original plant design.

Grounding

The MSFIS accepts 135 VDC (floating) input voltage. The PLC-5/25 power supplies provide 5 VDC to operate the A-B equipment. The A-B design provides all the internal grounding requirements for the PLC-5/25. The inputs are referenced to the 48 VDC power supply and are isolated from the 5 VDC.

Power

The MSFIS cabinets are supplied with Class IE 125 VDC power. This power source supplies the A-B equipment 5 VDC and the actuation relays 48 VDC. The power supplies are sized to handle the system loads. The ripple specification for the PLC-5/25 power supplies is +/- 10% and is satisfactory for the voltage quality delivered to the A-B equipment. Similarly, the 48 VDC ripple specification is +/- 10% and satisfactory for the actuation relays.

The MSFIS power supplies operate as required without producing spurious actuation or failure to produce a required response to accident conditions. A loss of power to a logic cabinet or applying power after a loss of power does not result in a MSFIS actuation. The loss of a power supply (5 VDC or 48 VDC) places the train in Bypass mode, which annunciates on the ESF status panel for each valve of that train. The operator takes action in accordance with the Operator Aid procedures, OOA-SA-C066X and OOA-SA-C066Y for ESF Status Panels SA066X and SA066Y Alarm Information.

Testability

The MSFIS can be tested during operation or shutdown, from a test panel located in each train cabinet. The Test Panel allows technicians to put a single train in test. The new Test Panel is similar to the existing Test Panel. All the existing test functions will be accomplished with the added ability to perform coincidence testing. The RPS slave relays that input either a Feedwater or Main Steam Isolation Signal can be tested by selecting the "Test Enable" function for any valve. This function ensures the actuation relay outputs are bypassed to prevent actual valve motion during the test. When any valve is put in "Test Enable", that valve status change is annunciated on the MCB ESF Status Panel. Only one train is tested at a time.

Since the MSFIS modification utilizes triple redundant logic, coincident testing is required. The coincident testing is accomplished by use of the application software and the hardware located at the Test Panel. The Read Test Panel program, which reads two channels at a time, generates the ESFAS input, which verifies that each set of logic channels trip to satisfy the two out of three logic design. This software undergoes the same V&V as previously described.

In order to prevent unauthorized entries or alterations of the MSFIS application software, the PLC-5 is configured with the "write" jumper removed from the processor. The "write" jumper is

controlled as part of the configuration management provided in procedure EDP-ZZ-04056, "Development and Configuration Control of Digital Plant Systems". Thus, the technician cannot change the operating code or reconfigure algorithms. In addition, the cabinets are locked and the keys are administratively controlled.

PLC Equipment Failure

If a PLC channel failure occurs due to a malfunction from the processor and/or input and output modules, a MSFIS A/B Channel Failure window will light on the main annunciator and at the MSFIS cabinet test panel. Self-testing is accomplished as part of the PLC-5 features. After each scan of the processor (~140 msec), the self-test program runs, and if a fault is detected the Channel Failure annunciator will light. The operator will take actions in accordance with the annunciator response procedures, OTA-RL-RK043 (Windows 43A-43F) and OTA-RL-RK044 (Windows 44A-44F). If either window goes into alarm, the operator must go to the respective cabinet, SA075 A or B, to determine which PLC has faulted. The Instrument and Controls Department will be alerted to correct the problem. If more than one PLC per train has faulted, Operations must take appropriate actions per Technical Specification Table 3.3-3.

Defense in Depth

The SSPS is designed using diverse techniques to achieve a high level of reliability to ensure that normal operating, maintenance, and postulated accident conditions do not result in the loss of a protection function. The SSPS will not be changed by this modification.

The MSFIS replacement equipment has a two out of three logic design that is more reliable than the existing single logic design. The A-B equipment, processors and input/output modules have sufficient field operating experience to estimate the MTBF (calculated at $>10^6$ Hrs by A-B). The existing system has a lower reliability (calculated at $> 10^5$ Hrs by Consolidated Controls - OEM).

The design of the software has undergone an extensive V&V process by SP, as previously stated. SP has provided digital upgrade equipment and similar PLC software for other nuclear plant applications. Also, SP has experience with an established software life cycle process that conforms to IEEE 7-4.3.2. Thus, as a result of utilizing an extensive development process, SP has produced a software product of high quality and reliability. A common mode software failure could exist if both trains of PLCs have a simultaneous software malfunction and/or fault. This

potential failure would prevent the operator from manually fast closing (FC) the FIVs or MSIVs from the MCB. Diversity is one method of addressing this concern. In the event of a secondary cycle pipe rupture inside the containment, the main feedwater control valves (MFCV) (and associated bypass valve) provide a diverse backup to the FIV to limit the quantity for high energy fluid that enters the containment through the broken loop.

A diverse means to operate the MSIVs is currently not available. Therefore, the MSFIS train cabinet will have an MSIV Fast Closure toggle switch added for each valve to allow manual operator action in the event of a common mode software failure coincident with an accident requiring an MSIV closure. Control Room indicators (i.e., steamline pressure, containment pressure, SI, SG level, etc.) are available to permit manual mitigation of the accidents listed in Section 3 of this submittal, in the unlikely event of a common mode failure. Considering the high quality established throughout the equipment design process, the possibility of a common mode failure is reduced to a very low probability. Therefore, in the event of a common mode software failure, sufficient indication diverse from the MSFIS and procedural guidance from operating procedures exist for the operator to take manual action to mitigate the transients involved in the Callaway accident analysis. In MSIV cases, where backup protective functions or manual operator actions are credited, Union Electric has not performed detailed analytical modeling to determine if the response time of these functions or actions is consistent with that of the primary function being replaced. In most cases the modeled response times would not be met. However, these manual actions are considered backups, and the probability is low for an accident or transient coupled with a common mode failure.

A Failure Modes and Effects Analysis was performed by SP with their System Reliability Analysis. This document is proprietary and available for review on site. The results indicated that no single failure would produce the loss of a protective function. The MSFIS equipment performs self-tests at the end of each scan cycle. If any failures are diagnosed, a channel failure will occur and be annunciated. The PLCs have an internal watchdog timer (WDT) which will time-out and produce a channel failure if the processor is caught in a loop. However, if the processor halts due to a software failure, the internal WDT may not time out, therefore, an external watchdog timer has been added to time-out and alerts the operator with a channel failure.

Factory Testing

A Factory Acceptance Test will be performed by SP to verify that the MSFIS equipment will meet the accuracy and functional requirements of specification J-1065. UE personnel will witness portions of the testing and review any deficiency reports produced.

UE in conjunction with an SP representative, will perform the Site Acceptance Testing (SAT) once the equipment is installed.

Product History

The main vendors supplying the MSFIS equipment are A-B for both the PLC hardware and software, and ICOM for the software development tools.

The A-B PLC-5 series of programmable logic controllers have been used extensively and control roughly 50% of the PLC market. The PLC-5/25 was introduced in 1988 and sales to date have exceeded 25,000 units.

Since A-B provides these units commercially, SP will commercially dedicate the PLC 5/25 for the MSFIS application at Callaway in accordance with EPRI Guideline NP 5652. SP performed a receipt inspection of the hardware and checked it for functional attributes and critical characteristics. The software provided by A-B will be tested by SP to check the instructions and verify that no unintended functions are present. A ladder logic program will be written which tests each instruction in all modes, checks the results against expectation, and sets a bit if the test fails. All status bits will be checked for failure at the end of the test. Similar testing will be performed for new versions of software. The ICOM software, which was utilized to develop the source code offline, will also be commercially dedicated.

When A-B revises their equipment or issues product safety alerts, they notify their distributors who notify their purchasers. SP will perform a hazards analysis for the change, if required. This analysis ensures updates are transmitted to the customer when changes occur. ICOM transmits their revisions in a similar manner. A-B will be added to UE's Vendor Equipment Technical Information Program (VETIP).

A-B maintains design control of their product lines. A-B identifies the product need, reviews changes, and assigns a design review committee for implementation. Functional confirmation testing is performed on each product line. A-B maintains a qualified supplier list.

Hardware and software suppliers are added to SP's approved supplier list after a survey of the supplier quality process is completed. The survey focuses on the supplier quality assurance manual, if available, and their software life cycle processes. Each year, questionnaires are sent to the suppliers to provide management and/or process changes which might effect quality. Class 1E suppliers are surveyed every three years.

An A-B survey was completed by SP to thread through the development and manufacturing process (which is similar for the PLC 5/25 units) of the PLC 5/10 units. The results were acceptable, with an action to assure correct identification of PROM firmware revisions. As a result, a PROM reader was purchased and a receipt inspection procedure was established to "read" the PROM and perform a checksum. The replacement checksum is compared to the current PROM checksum.

ICOM was also surveyed by SP to verify their process for ladder logic editing, on-line communications for down loading, on-line editing, and PLC monitoring. The applications engineers act as verifiers and contact customers if any software problems arise that could affect them.

Training and Procedures

A number of procedures will be revised as a result of this modification. The effected procedures include surveillance, annunciator response, and operator aids.

SP will provide the operation and maintenance manual for the new system.

Training will be provided for the Instrumentation and Control, Engineering, and Operations Departments.

This modification is in the final design stages, and all open issues will be resolved by the completion of the modification. SP has forecast a final design and hardware shipment date of mid April 1996.

SECTION 3: FORMAL SAFETY EVALUATION

This section summarizes the safety evaluation that was performed to support the MSFIS modification.

MSFIS Modification

1. Will the proposed activity increase the probability of occurrence or the consequence of an accident or malfunction

of equipment important to safety previously evaluated in the safety analysis report?

The following design basis accidents rely upon Feedwater Isolation Valves and/or Main Steam Isolation Valves to close and mitigate their consequences:

- Feedwater system malfunction that results in an increase of feedwater flow
- Inadvertent opening of a steam generator relief or safety valve
- Steam system piping failure
- Loss of non-emergency AC power
- Loss of normal feedwater
- Feedwater system pipe break
- Steamline break in Area 5
- Steam Generator Tube Rupture
- Station Blackout/Loss of Coolant Accident

No design basis accidents will be affected by this design change since the logic that currently exists will continue to be performed. Thus, the radiological consequences will not change.

The system response time is enveloped by the current 5 second valve stroke time. The MSFIS response time will be less than 500 msec.

A common mode software failure could exist if both separation groups have their PLCs (3 per train - six total) malfunction at the same time. However, a diverse means of isolating the feedwater lines currently exists given the ability of the MFCVs to close on a Feedwater Isolation Signal. The MSIVs do not have a diverse means of isolating their respective steam lines if a common mode software failure occurs. As a result, this modification provides a means to manually fast close the valves at the MSFIS cabinets. The operators will be alerted of the failure conditions of any PLC logic channel via MCB annunciators and indicators. This failure mode has a low probability of occurrence based upon the inherent quality of the design provided by the V&V process. Therefore, the accident consequences are not increased for this failure mode.

The operator's ability to adequately respond to an accident is not hindered by the man-machine interface added as a result of this modification. The MCB controls will not change. The Test Panel operates similar to the existing test panel. Training will be provided to the technicians, engineers, and operators on the

new features of the system prior to installation. Therefore, this modification does not increase the consequential effects due to the man-machine interface.

The replacement system is functionally the same as the current system since it performs the same logic, receives the same inputs, and produces the same outputs. However, the system is more reliable and possesses triple redundant logic. The value for the MTBF as listed in SP's System Reliability Analysis is $>10^6$ Hrs. The V&V program assures that the system software is of a high quality. Thus, the probability of malfunction will not be increased.

Operator interface is similar to the current system by permitting operator inputs at the MCB and receiving the appropriate valve actions. During abnormal conditions, such as a common mode software failure coincident with an MSIV closure, the operator will have to close the MSIVs with switches located on an Emergency Override Panel. This manual action will not increase the probability of any accidents analyzed.

Proper grounding is provided for the PLC 5 VDC and actuation relay 48 VDC power supplies, which are electrically isolated from each other.

The operators will be alerted to system malfunctions through annunciation. The current system has a status output for each MSIV and FIV on the Engineered Safety Feature Status Panel, which will be maintained. In addition, an isolated plant annunciator interface will provide a MSFIS Channel Failure plant annunciator window for both trains.

The electrical load of the A-B PLC equipment and existing 48 VDC actuation relays is less than that of the existing equipment. Therefore, the system will not require any additional cooling over the existing equipment.

For the previous reasons, the proposed activity will not increase the probability or consequences of a malfunction of equipment important to safety.

2. Will the proposed activity create the possibility for an accident or malfunction of a different type than any previously evaluated in the safety analysis report?

The system is compatible with the normal and accident environments (i.e., temperature, humidity, seismic and electromagnetic). The equipment will be qualified seismically in accordance with the SNUPPS seismic spectra profile. The

equipment will be qualified for Electromagnetic Interference concerns in accordance with EPRI document TR-102323-EPRI Guideline and will meet the EPRI EMI limiting practices.

The system has the same failure mode upon loss of power as the current system and behaves similarly upon power restoration. A loss of power will not result in a MSFIS actuation. Any reset or repowering of the equipment will reset the processor which initiates a new scan cycle so that the inputs are all "read", the logic executed and the outputs "written".

The man-machine interface will not introduce failure modes different from the existing system. The MSFIS cabinet test panel has been laid out to provide the same functions as the existing test panel, except that PLC status indication and coincidence logic test functions are also provided. The Emergency Override Panel, located at the back of the cabinet, provides the operator with the ability to bypass the FWIS and manually fast close each MSIV as required per the Emergency Operating Procedures. The FWIS bypass switch function will allow main feedwater flow to be re-established to each Steam Generator. The MSIV manual FC switch operation is necessary for a diverse means of operation for software common mode failures.

There are three items associated with the MSFIS replacement equipment that may result in an unreviewed safety question:

a. Identical PLCs are utilized in the MSFIS design change which introduces the potential for a common mode failure of the software that the PLCs will utilize.

b. The original NRC review of MSFIS did not evaluate a 2 out of 3 coincidence circuit for MSFIS actuation; therefore, a potential unreviewed safety question exists because new failure modes could be present.

c. The design change incorporates manual handswitches that bypass the MSIV/FIV circuits. The handswitches potentially involve a new failure mode that was not originally addressed in the FSAR.

Even though this design change is an improvement over the existing equipment, the above items lead to the conclusion that this change constitutes an unreviewed safety question.

3. Will the proposed activity reduce the margin of safety as defined in the basis for any technical specification?

Since no setpoints are revised, the system will not reduce the margin of safety as defined in the basis for any Technical Specification.

The system response time for any given valve will not exceed the required actuation time.

The MSFIS does not contain any analog channels, therefore, no channel trip accuracys are impacted.

Justification for Approval of Proposed Modification

The types of digital equipment designs, malfunctions, and failure modes listed in Question 2 above have been evaluated by NRC for other plant digital upgrades. The Callaway PLC design, common mode failure potential, and use of MSIV/FIV FC toggle handswitches do not produce a safety concern as discussed below.

The new system performs the same logic as the existing system for the same accidents, but with added reliability because of the triple redundant logic. Each MSFIS train has 3 PLCs. The inputs are triplicated, sent to triplicate PLCs to perform the valve logic, and outputted in triplicate into a 2 out of 3 relay hardwired logic. If one PLC fails in a given train, that logic will revert to a 2 out of 2 logic. When a PLC fails or has detected a fault, all outputs go to the standby state for that PLC. This means that the PLC output contacts are left in an open state and do not produce a trip condition. However, the remaining two logic channels satisfy the two sets of output contacts required to produce a relay actuation.

The use of identical PLCs for this application introduces the potential for a common mode failure. The common mode failure is different from the equipment malfunctions previously evaluated in the FSAR; however, a diverse means of operation will exist for this malfunction. The Defense in Depth Analysis provided in Section 2 of this submittal supports this position. Sufficient indication, diverse from the MSFIS, and procedural guidance from operating procedures, exist for the operator to take manual actions to mitigate the transients analyzed in the Callaway accident analysis. The probability is low for an accident or transient coupled with a common mode software failure that does not fail into the preferred state.

No new types of failure modes will be generated, even with the addition of the FIV bypass and MSIV manual fast close toggle switches, that will create different types of accidents than previously evaluated in the FSAR.

The new equipment will not create any new EMI environmental problems nor be impacted by the environment to cause a different type of malfunction than previously evaluated.

Description of Technical Specification Change and Evaluation

The license amendment requests a revision to Technical Specification 3/4.3.2 "Engineered Safety Features Actuation System Instrumentation." This specification is revised by the addition of the MSFIS actuation logic and relays to Functional Units 4.b and 5.a of Tables 3.3-3, 3.3-4 and 4.3-2. Table 3.3-3 is further revised by the addition of Action Statements 27a and 34a, which provide guidance in the event of an inoperable MSFIS channel or train. The requirements of these Action Statements are specific for the MSFIS and consistent with the requirements of SSPS Action Statements 27 and 34.

Conclusion

Considering the information presented above, the proposed modification and TS changes do not present a safety concern and are therefore justified since they will not adversely effect the health and safety of the public.

FIGURE 1

MSIV and FIV Valves
Current System

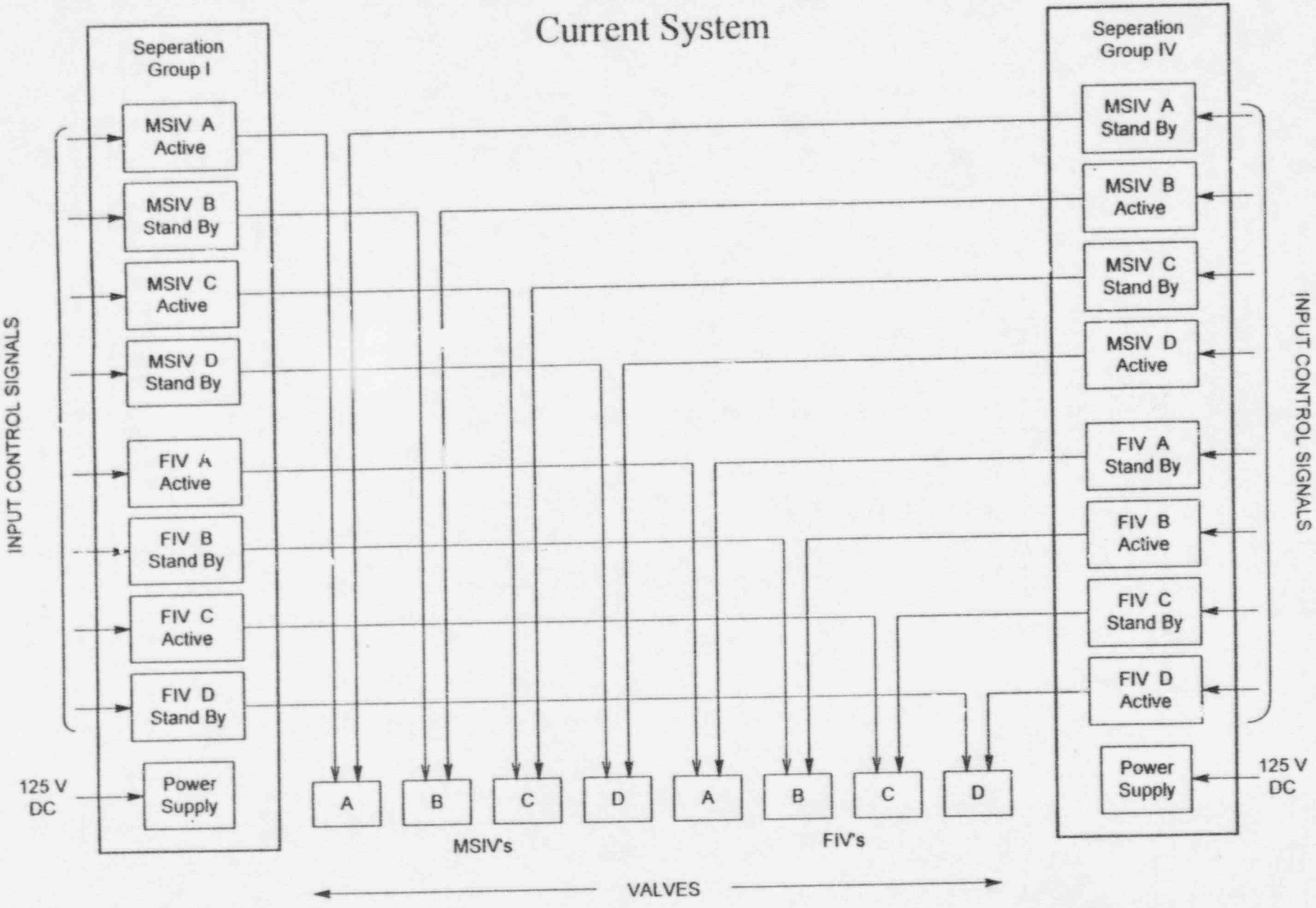
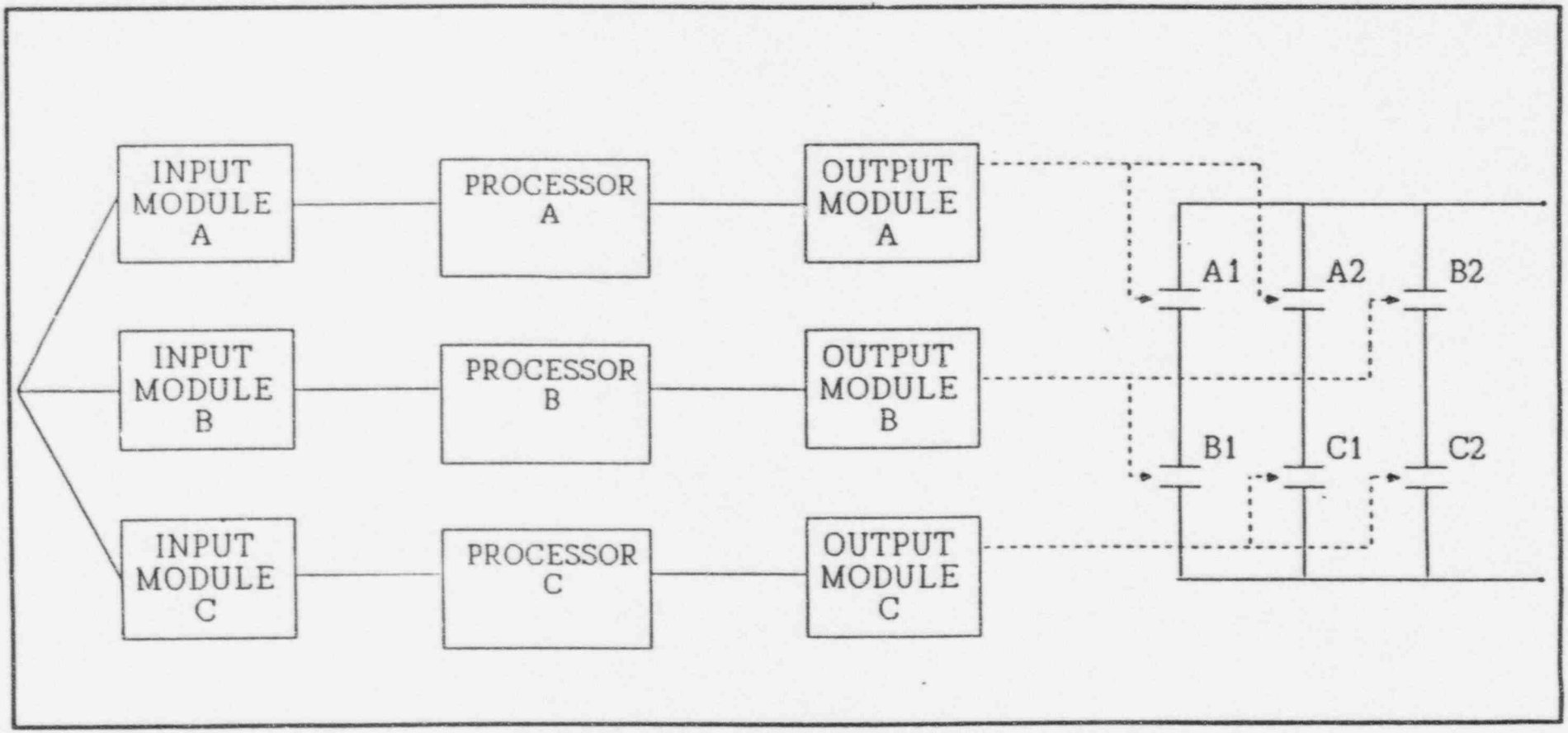
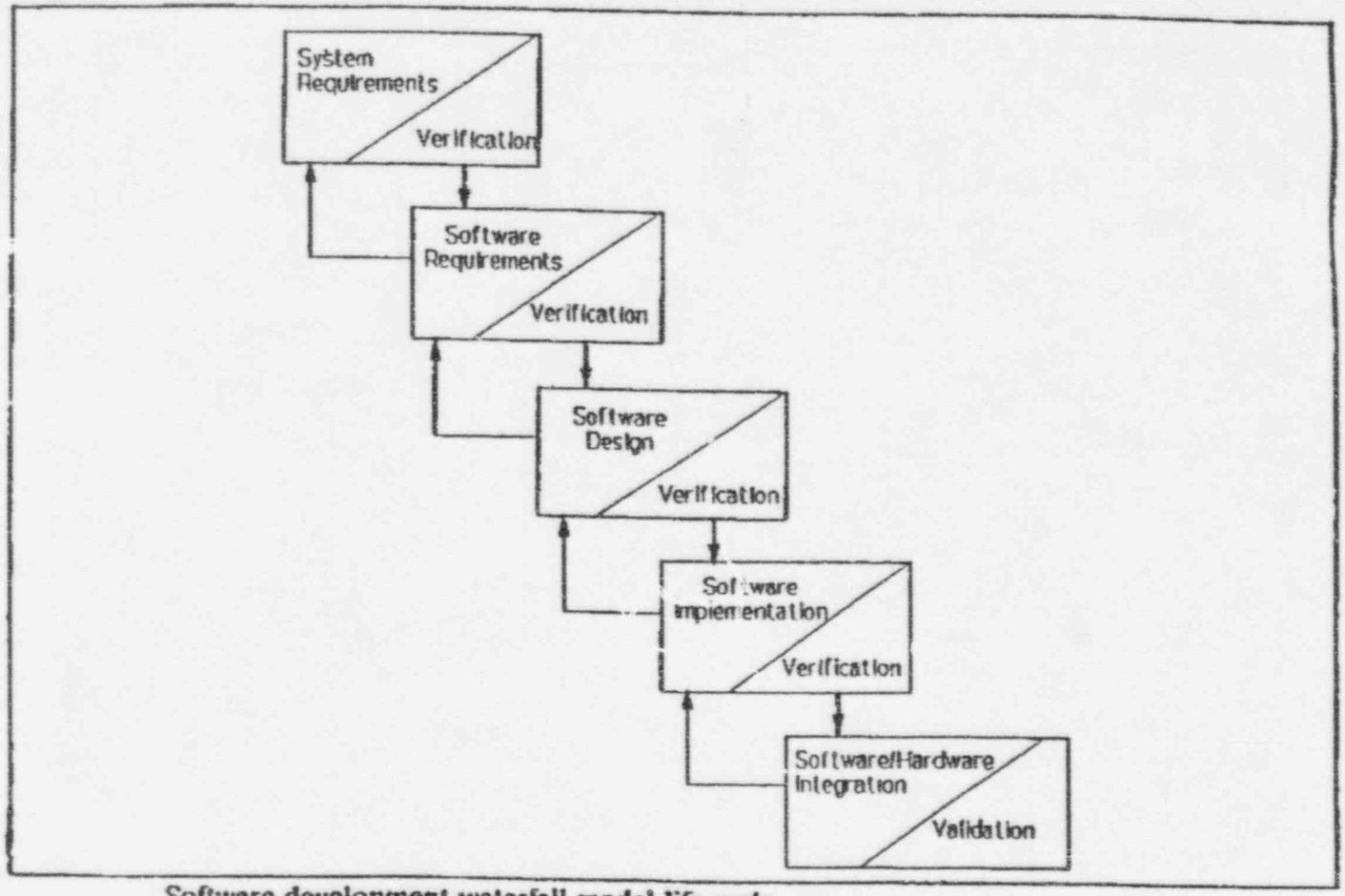


FIGURE 2



Two-out-of-three voting with three independent processors

FIGURE 3



Software development waterfall model life cycle

ATTACHMENT 4

SIGNIFICANT HAZARDS EVALUATION

SIGNIFICANT HAZARDS EVALUATION

Introduction

This license amendment requests a revision to Technical Specification (TS) 3/4.3.2 "Engineered Safety Features Actuation System Instrumentation". This specification is revised by adding the Main Steam and Feedwater Isolation System (MSFIS) actuation logic and relays to Functional Units 4.b and 5.a of Tables 3.3-3, 3.3-4, and 4.3-2. Table 3.3-3 is further revised by the addition of Action Statements 27a and 34a, which provide guidance in the event of an inoperable MSFIS channel or train. These proposed changes are the result of a modification that will replace existing digital portions of the MSFIS with digital processor equipment.

The existing MSFIS logic is considered part of the Solid State Protection System (SSPS) in TS. Currently, if one train of MSFIS is inoperable, then one train of SSPS is inoperable. The modified MSFIS has a two out of three logic design for each train. The addition of MSFIS actuation logic and relays to TS Tables 3.3-3, 3.3-4, and 4.3-2 allows one channel of MSFIS to be declared inoperable or placed in test without declaring the corresponding train of SSPS inoperable.

Background

The MSFIS consists of two independent actuation trains that monitor system inputs and by means of logic matrices, drive actuation relays that energize or deenergize the solenoids required for the appropriate Main Steam or Main Feedwater Isolation Valve operation.

The modified MSFIS performs the same as the current design except the system is comprised of triple redundant logic consisting of three logic channels in two different trains. The SSPS and Reactor Protection System inputs the Engineered Safety Features Actuation System signals, the Main Control Board handswitches input to the MSFIS cabinets, and the same actuation output relays are utilized for the new design.

Justification for Approval of Proposed Change

The types of digital equipment designs, malfunctions, and failure modes have been evaluated by NRC for other plant digital upgrades. For the reasons listed below, the PLC design, common

mode failure potential and assessment of MSIV/MFIV FC toggle handswitches do not produce a safety concern.

The new system performs the same logic as the existing system for the same accidents, but with added reliability because of the triple redundant logic. The inputs are triplicated, sent to triplicate PLCs to perform the valve logic, and outputted in triplicate into a 2 out of 3 relay hardwired logic. If one PLC fails in a given train, that logic will revert to a 2 out of 2 logic. When a PLC fails or has detected a fault, all outputs go to the standby state for that PLC. This means that the PLC output contacts are left in an open state and do not produce a trip condition. Therfore, the remaining two logic channels satisfy the two sets of output contacts required to produce a relay actuation.

The use of identical PLCs for this application introduces the potential for a common mode failure different than the equipment malfunctions previously evaluated in the FSAR; however, a diverse means of operation exists for this malfunction. Indication, diverse from the MSFIS, and procedural guidance, exist for the operator to take manual actions to mitigate the transients analyzed in the Callaway accident analysis. The probability is low for an accident or transient coupled with a common mode software failure that does not fail into the preferred state.

No new types of failure modes will be generated, even with the addition of the FIV bypass and MSIV manual fast close toggle switches, that will create different types of accidents than previously evaluated in the FSAR.

The new equipment will not create any new EMI environmental problems nor be impacted by the existing environment to cause a different type of malfunction than previously evaluated.

Evaluation

The proposed changes to the plant and to TS do not involve a significant hazards consideration because operation of Callaway Plant with these changes would not:

1. Involve a significant increase in the probability of occurrence or the consequences of an accident or malfunction of equipment important to safety previously evaluated in the Safety Analysis Report.

The addition of the MSFIS actuation logic and relays to the TS has no adverse impact on the probability of occurrence or the consequences of an accident. The proposed amendment does not change or alter the design assumptions for the systems or components used to mitigate the consequences of an accident and the methodologies used in the accident analysis remain unchanged. The operating limits will not be changed.

No design basis accidents will be affected by this design change since the logic which currently exists will continue to be performed. Thus, the radiological consequences will not change.

The system response time is enveloped by the current 5 second valve stroke time. The MSFIS response time will be less than 500 msec.

A common mode software failure could exist if both separation groups have their PLCs (3 per train - six total) malfunction at the same time. However, a diverse means of isolating the feedwater lines exists given the ability of the Main Feed Control Valves to close on a Feedwater Isolation Signal. The MSIVs do not have a diverse means of isolating their respective steam lines if a common mode software failure occurs. As a result, this modification provides a means to manually fast close the valves at the MSFIS cabinets. The operators will be alerted of the failure conditions of any PLC logic channel via MCB annunciators and indicators. This failure mode has a low probability of occurrence based upon the inherent quality of the design provided by the V&V process. Therefore, the accident consequences are not increased for this failure mode.

The test panel in the MSFIS cabinets has been laid out to provide the same functions as the existing test panel, except that PLC status indication and coincidence logic test functions are provided. The Emergency Override Panel, located below the Test Panel, provides the operator with the ability to bypass the FWIS signal and manually fast close each MSIV as required by the Emergency Operating Procedures. The MSIV manual FC switch operation is necessary for a diverse means of operation for software common mode failures. The FWIS bypass switch will allow main feedwater flow to be re-established to each Steam Generator.

The replacement system is functionally the same as the current system since it performs the same logic, receives the same inputs, and produces the same outputs. However, the system is more reliable and possesses triple redundant logic. Therefore, the probability of malfunction will not be increased.

The electrical load of the A-B PLC equipment and existing 48 VDC actuation relays is less than that of the existing equipment so the system will not require any additional cooling over the existing equipment. Proper grounding is provided for the PLC 5 VDC and actuation relay 48 VDC power supplies, which are electrically isolated from each other.

2. Create the possibility of a new or different kind of accident from any previously evaluated in the Safety Analysis Report.

The addition of the MSFIS actuation logic and relays to the TS will not create a new type of accident or malfunction than any previously evaluated in the Safety Analysis Report. The safety functions of the system are not changed in any manner, nor is the reliability of any structure, system or component reduced. All design and performance criteria continue to be met. Since the safety functions and reliability are not adversely affected, the proposed change does not create the possibility of a new or different kind of accident from any accident previously evaluated.

The operator's ability to adequately respond to an accident is not hindered by the man-machine interface added as a result of this modification since the operator interface is similar to the current system and the MCB controls will not change. The operators will be alerted to system malfunctions through annunciation. The current system has a status output for each MSIV and FIV valve on the Engineered Safety Feature Status Panel, which will be maintained. In addition, an isolated plant annunciator interface will provide a MSFIS Channel Failure plant annunciator window for both trains. Training will be provided to the technicians, engineers, and operators on the new features of the system prior to installation. Therefore, this modification does not increase the consequential effects due to the man-machine interface.

The system is compatible with the normal and accident environments and will be seismically qualified in accordance with the SNUPPS seismic spectra profile. The equipment will be qualified for Electromagnetic Interference concerns in accordance with EPRI document TR-102323-EPRI Guideline and will meet the EPRI EMI limiting practices.

The system has the same failure mode upon loss of power as the current system and behaves similarly upon power restoration. A loss of power will not result in a MSFIS actuation.

3. Involve a significant reduction in a margin of safety.

The addition of the MSFIS actuation logic and relays to the TS will not affect or change a safety limit or affect plant operations. This change will not reduce the margin of safety assumed in the accident analysis nor reduce any margin of safety as defined in the basis for any TS.

The system response time for any given valve will not exceed the required valve stroke time. Since the MSFIS does not contain any analog channels, no channel trip accuracies are impacted

Conclusion

Given the above discussions, the proposed change does not adversely affect or endanger the health or safety of the general public or involve a significant hazards consideration.

ATTACHMENT 5

ENVIRONMENTAL CONSIDERATION

ENVIRONMENTAL CONSIDERATION

This license amendment requests a revision to Technical Specification (TS) 3/4.3.2 "Engineered Safety Features Actuation System Instrumentation". This specification is revised by adding the Main Steam and Feedwater Isolation System (MSFIS) actuation logic and relays to Functional Units 4.b and 5.a of Tables 3.3-3, 3.3-4, and 4.3-2. Table 3.3-3 is further revised by the addition of Action Statements 27a and 34a, which provide guidance in the event of an inoperable MSFIS channel or train. These proposed changes are the result of a modification which will replace existing digital portions of the MSFIS with digital processor equipment.

The proposed amendment involves changes with respect to the use of facility components located within the restricted area, as defined in 10 CFR 20. Union Electric has determined that the proposed amendment does not involve:

(1) A significant hazard consideration, as discussed in Attachment 4 of this amendment application;

(2) A significant change in the types or significant increase in the amounts of any effluents that may be released offsite;

(3) A significant increase in individual or cumulative occupational radiation exposure, as discussed in Attachment 3 of this amendment application.

Accordingly, the proposed amendment meets the eligibility criteria for categorical exclusion set forth in 10 CFR 51.22(c)(9). Pursuant to 10 CFR 51.22(b), no environmental impact statement or enviromental assessment need be prepared in connection with the issuance of this amendment.