Pressurized Water Reactor
B&W Technology
Crosstraining Course Manual

Chapter 10.2

Engineered Safety Features Actuation System

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

This page intentionally blank.

10.2 ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

Learning Objectives:

1. List the functions provided by the engineered safety features actuation system (ESFAS).

2. List the ESFAS signals and the accidents that will initiate each.

3. Define the following terms:

    a. Analog subsystem
    b. Digital subsystem
    c. ESFAS channel
    d. Unit control module

4. Describe the sequence of events (flowpath) for an ESFAS signal from the sensor to component actuation, including ESFAS logic.

5. List the systems that are actuated by ESFAS signals.

6. Explain when and how the ESFAS is bypassed.

7. Explain how the control room operator gains equipment control after an ESFAS actuation has occurred.

8. Describe the status of the ESFAS following the loss of one train of the vital 120-Vac distribution system.

9. Describe the purpose of the Secondary Protection System and explain how that purpose is accomplished.

10.2.1 Introduction

The engineered safety features actuation system is designed to actuate emergency core cooling system equipment, reactor building isolation valves, and reactor building pressure control equipment. The components are activated by the ESFAS in the event of a loss-of-coolant accident, steamline break, or feedwater line break, and perform the following functions:

1. Minimize fuel cladding damage,
2. Provide reactor building isolation,
3. Decrease reactor building pressure,

4. Remove fission products from the reactor building atmosphere, and
5. Provide long-term core cooling.

10.2.2 System Description

To accomplish the required functions, the ESFAS is supplied with various pressure and level transmitter inputs that are used as indications of accident conditions. By sensing reactor coolant pressure, reactor building pressure, and BWST level, ESFAS can actuate emergency equipment that will mitigate the consequences of primary or secondary system line breaks.

If a rupture occurs in the reactor coolant system (RCS), reactor coolant pressure will decrease and reactor building pressure will increase. Also, if a main steamline breaks inside the reactor building, reactor coolant pressure will decrease because of overcooling of the RCS, and reactor building pressure will increase. A steamline break outside the reactor building will also produce an RCS pressure decrease, but this break will not cause an increase in reactor building pressure. If the feedwater header breaks inside the reactor building, the hot feedwater will flash to steam. The flashing of feedwater coupled with the blowdown of the steam generator will increase reactor building pressure. By comparing the changes in pressures with predetermined setpoints, the ESFAS can actuate the necessary emergency systems.

The required comparison of input pressures with predetermined setpoints is performed in three separate, redundant analog ESFAS subsystems (Figure 10.2-1). If any two of these three subsystems sense that an input pressure parameter has reached its setpoint, two redundant digital subsystems will be activated by the analog subsystems. The digital subsystems provide start-stop/open-close signals to the redundant engineered safety features (ESF) equipment. The ESF equipment is divided almost equally between the digital cabinets so that in the event of a failure of a digital subsystem, the operable digital subsystem will initiate the operation of sufficient equipment to mitigate the effects of the accident.

The basic actuation scheme of the ESFAS is that when pressures in two out of three analog subsystems reach their setpoint, they de-energize relays that, in turn, energize the digital subsystems. Table 10.2-1 shows a listing of the analog inputs and setpoints, the digital subsystem channel divisions, and the emergency systems that are actuated by the redundant (A and B) digital subsystems.

10.2.3 Analog Inputs

10.2.3.1 Reactor Coolant System Pressure

The reactor coolant pressure inputs to the ESFAS originate with pressure transmitters that sense RCS hot-leg pressure. Three wide-range (0 - 2500 psig) transmitters (two

sense loop A pressure, and one senses loop B pressure) provide the required inputs (one transmitter for each ESFAS analog subsystem).

10.2.3.2 Reactor Building Pressure

A separate reactor building pressure transmitter with a range of -5 to +35 psig provides an input to each ESFAS analog subsystem.

10.2.3.3 Borated Water Storage Tank Level

Each individual analog subsystem receives a 0 – 55 feet borated water storage tank (BWST) level input from a separate level transmitter.

10.2.4 Analog Subsystems

There are three redundant analog subsystems (Figure 10.2-2). The subsystems are separate, redundant sets of pressure and level sensors and bistables. The bistable de-energize (i.e., trip) when their individual predetermined setpoints are reached. A tripped bistable sends an actuation signal to both digital subsystems. A single typical analog subsystem is discussed in the following section.

10.2.4.1 Input Signal Processing

Each of the transmitters associated with the analog subassembly supplies its input through a buffer amplifier. This buffer converts the 4 – 20 ma transmitter signal to a 0 – 10 vdc signal. The output of the buffer is supplied to a meter that locally displays the value of the parameter at the ESF cabinets and to bistable(s) for ESF actuation.

10.2.4.2 Bistables

Each analog subsystem bistable receives two inputs, the actual value of the parameter and the predetermined setpoint, and compares the two. If the actual parameter reaches the setpoint, the bistable will trip. Bistable tripping is indicative of the need for emergency system actuation. The outputs of the high-high reactor building (RB) pressure bistables and the low BWST level bistable are connected directly to logic buffers. The outputs of the low RCS pressure and the high RB pressure bistables are connected to “OR” gates.

10.2.4.3 Emergency Core Cooling Initiation

Emergency core cooling initiation (ECCI) is initiated from the low RCS pressure bistable and the high RB pressure bistable. If either of these bistables trip, the ECCI “OR” gate will transmit an actuation signal to the digital subsytems’ logic gates.

10.2.4.4 Reactor Building Isolation

Reactor building isolation is initiated from the high RB pressure bistable or the low RCS pressure bistable. If either of these bistables trip, the RB isolation "OR" gate will transmit an actuation signal to the digital subsytems' logic gates.

10.2.4.5 Reactor Building Spray

Reactor building spray is initiated from two high-high (>25 psig) bistables. Two bistables are used to minimize the possibility of inadvertent spray addition to the RB atmosphere.

10.2.4.6 Sump Recirculation

Sump recirculation is initiated by low BWST level. The purpose of this signal is to provide automatic alignment of long-term core cooling.

10.2.5 Digital Subsystems

The digital subsystems are separate, redundant sets of logic gates which receive input signals from the three redundant analog subsystems and sends actuation signals to the unit control modules. When the digital subsystems sense that any two of the three analog subsystems have de-energized, the digital subsystems will energize to activate engineered safety features equipment.

10.2.5.1 Two-out-of-Three Digital Logic

The outputs of the analog subassemblies are connected to the 2-out-of-3 logic gates in the digital subassemblies. These logic gates represent all possible 2-out-of-3 combinations (AB, AC, BC). The output of each logic gate is connected to the unit control modules associated with the digital channel. If any two out of three analog subsystems de-energize, the associated 2-out-of-3 logic gate will energize and actuate the unit control modules.

10.2.5.2 Unit Control Modules

The unit control modules serve as the interface devices between the ESFAS and the emergency equipment. There is a unit control module installed for each piece of emergency equipment required to be operated. When the unit control modules are energized, relay action starts the required pumps and opens or closes valves to align the emergency systems for the accident condition. The actuation of equipment by the unit control module bypasses the normal control switch (start/stop, open/close) for the emergency equipment. Manual and automatic pushbuttons are provided for each unit control module and are discussed in Section 10.2.6.2.

10.2.6 Manual Initiation and Bypass

10.2.6.1 Manual Initiation

The operator can manually initiate ESFAS if deemed necessary or if a failure of the analog subsystems occurs. A manual initiation switch (Figure 10.2-2) is installed for each digital channel and is connected to a digital logic "OR" gate. When the manual switch is depressed, it will cause the "OR" gate to energize the unit control modules. The action of the unit control modules is the same as that initiated by an automatic signal.

A manual reset switch (not shown) is also installed for each digital channel. This switch allows the resetting of the digital "OR" gate after manual initiation. Manual resetting of the system can be accomplished only if no automatic actuation signal is present. The manual reset switch will not override the automatic actuation caused by the analog subsystems, reposition any valves, or stop any pumps.

10.2.6.2 Unit Control Module Operation

The manual and automatic pushbuttons (Figure 10.2-3) associated with a unit control module allow (1) manual control of the particular emergency system component controlled by that unit control module, (2) the return of the emergency equipment to automatic control, and (3) the testing of emergency system component response to an ESFAS signal.

If an ESFAS signal has actuated the emergency systems, the operator can regain control of an individual component by first depressing the manual pushbutton of the associated unit control module and then changing the condition (i.e., on or off, open or closed) of the component with its normal control switch. The manual and automatic pushbuttons only affect the unit control module logic. Therefore, only the associated components are affected when the manual pushbutton is depressed. The operator can return the components to their accident positions by depressing the automatic pushbutton of the appropriate unit control module.

The final function of the manual and automatic pushbuttons is component testing. During certain portions of ESFAS testing, power to the internal logic of the unit control module is provided by an energized test bus. In this situation, an emergency system component can be made to assume its accident position by depressing the manual pushbutton. The test would be ended by depressing the automatic pushbutton.

10.2.6.3 Bypass Circuits

During normal plant cooldowns, RCS temperature and pressure are reduced. To prevent inadvertent ESFAS actuation, low RCS pressure actuation can be bypassed (Figure 10.2-2). When RCS pressure is less than 1850 psig, as sensed by the RCS pressure bypass bistables, the operator is allowed to bypass the RCS pressure inputs to the emergency core cooling initiation and RB isolation "OR" gates. As the plant is heated

up and RCS pressure is increased to above 1850 psig, the bypass is automatically removed.

10.2.7 System Operations

10.2.7.1 Decay Heat Removal Valve Interlocks

The reactor coolant system pressure transmitters are connected to bistables that provide interlocks for valve positions in the decay heat removal (DHR) system. The DHR suction isolation valves are interlocked closed on high RCS pressure to prevent exceeding the design pressure of the DHR system. The DHR suction line originates from the loop "A" hot leg and then splits into two separate 14-inch pipes. Each of these pipes contains two motor-operated isolation valves. One valve in each suction pipe is automatically closed by ESFAS, and the other valve is closed by the essential controls and instrumentation system. The DHR valve interlock is supplied from analog subsystems A and B.

10.2.7.2 Sump Recirculation Channel Interlocks

During plant cooldowns, the suctions for the low-pressure injection system are aligned to the A RCS hot leg. During this time, the automatic switchover to the reactor building sump for long-term core cooling could damage the decay heat removal pumps. To prevent the automatic switchover, the sump recirculation ESFAS channels (5A and 5B) are interlocked with channels 1A and 1B. Since bypass is initiated during cooldown, channels 1A and 1B cannot actuate, and automatic switchover of the low-pressure injection suctions to the reactor building sump is prevented. This feature is of particular importance when the BWST contents are pumped to the refueling canal during refueling.

10.2.7.3 Loss of One Vital AC Power Source

The ESFAS receives power from 120-vac class 1E vital busses. However, one analog (A) and one digital subsystem (A) receive power from the same vital bus. The ability of the system to function during a loss of this power source is discussed below.

When power is lost to analog subsystem A, all the bistables (Figure 10.2-2) associated with this subsystem will de-energize. Digital subsystem B will receive an analog subsystem A actuation input in each digital channel. Digital subsystem A will be inoperable because it is an energize-to-operate subsystem.

The status of the ESFAS will be as follows:

1. Analog subsystem A bistables are all de-energized, sending actuation signals to digital subsystems A and B.

2. Digital subsystem B actuation logic has been reduced to 1-out-of-2, and the remaining required signal to actuate must originate in analog subsystem B or C.

3. Only the emergency equipment that is controlled by digital subsystem B will automatically actuate if a valid signal is received. However, since the emergency equipment is redundant, only one-half of the emergency equipment is required to actuate to provide protection for any accident. The loss of digital subsystem A does not interfere with the manual starting of emergency equipment by the operator.

10.2.8 PRA Insights

There is a failure probability associated with the ESFAS system. However, the possibility of mis-calibration of instrumentation or misreading of instrumentation (human error) outweighs the possibility of hardware failure, according to the ANO1 PRA. The relative importance of the failure of ESFAS to core melt is low, according to generic PWR PRA data. In fact, the system ranks 14th out of 15 systems in order of importance.

10.2.9 Secondary Protection System

If a break occurs in the secondary system, the accident is mitigated by the closure of main steam isolation valves (MSIVs) and main feedwater isolation valves (MFIVs). A break in a steamline upstream of the MSIVs will result in a pressure decrease in at least one steam generator. The Secondary Protection System will close the affected steam generator's MSIVs and MFIVs, trip both MFPs, and send a start signal to the AFW pumps when pressure is less than 800 psig (Figure 10.2-4). This action and the operation of the feed-only-good-generator logic of the auxiliary feedwater system, described in Chapter 5, will limit the blowdown to that of one steam generator. A break downstream of the MSIVs, which depressurizes both steam generators, will result in closure of all MSIVs and MFIVs, isolating the break. A high-high reactor building pressure (25 psig) will also close all the MSIVs and MFIVs. Table 10.2-2 shows the components actuated by the different channels and sub-channels.

Actuation of the Secondary Protection System can be bypassed for normal cooldown and depressurization when steam generator pressure is less than 900 psig. Bypassing the Secondary Protection requires manual action by the operator for each steam generator separately. Secondary Protection is automatically reset for each steam generator when pressure exceeds 900 psig.

10.2.10 Summary

The engineered safety features actuation system (ESFAS) is designed to aid in the mitigation of primary and secondary system breaks by sensing the abnormal condition and actuating emergency equipment. In addition, the ESFAS provides long-term core cooling during a loss-of-coolant accident by shifting the suctions of the emergency core cooling pumps from the BWST to the decay heat removal (DHR) recirculation sump.

The ESFAS consists of three separate, redundant analog subsystems, which are de-energized to actuate, and two separate, redundant digital subsystems, which are energized to actuate. The analog subsystems receive inputs of RCS pressure, RB pressure, and BWST level and compare these inputs with predetermined setpoints to ascertain the need for emergency system operation. The digital subsystems receive inputs from the analog subsystems, and if at least 2 out of 3 analog subsystems have reached a setpoint, then actuation of emergency equipment will occur. Each digital subsystem is divided into redundant channels that control different functions. The first channel actuates high-pressure injection and low-pressure injection on low RCS or high RB pressure. The second channel activates RB isolation on low RCS pressure or high RB pressure. The third and fourth digital channels actuate the RB spray header isolation valves and RB spray pumps on high-high RB pressure. The final channel is provided to accomplish the automatic emergency core cooling system suction switchover from the BWST to the DHR recirculation sump when a low level condition occurs in the BWST.

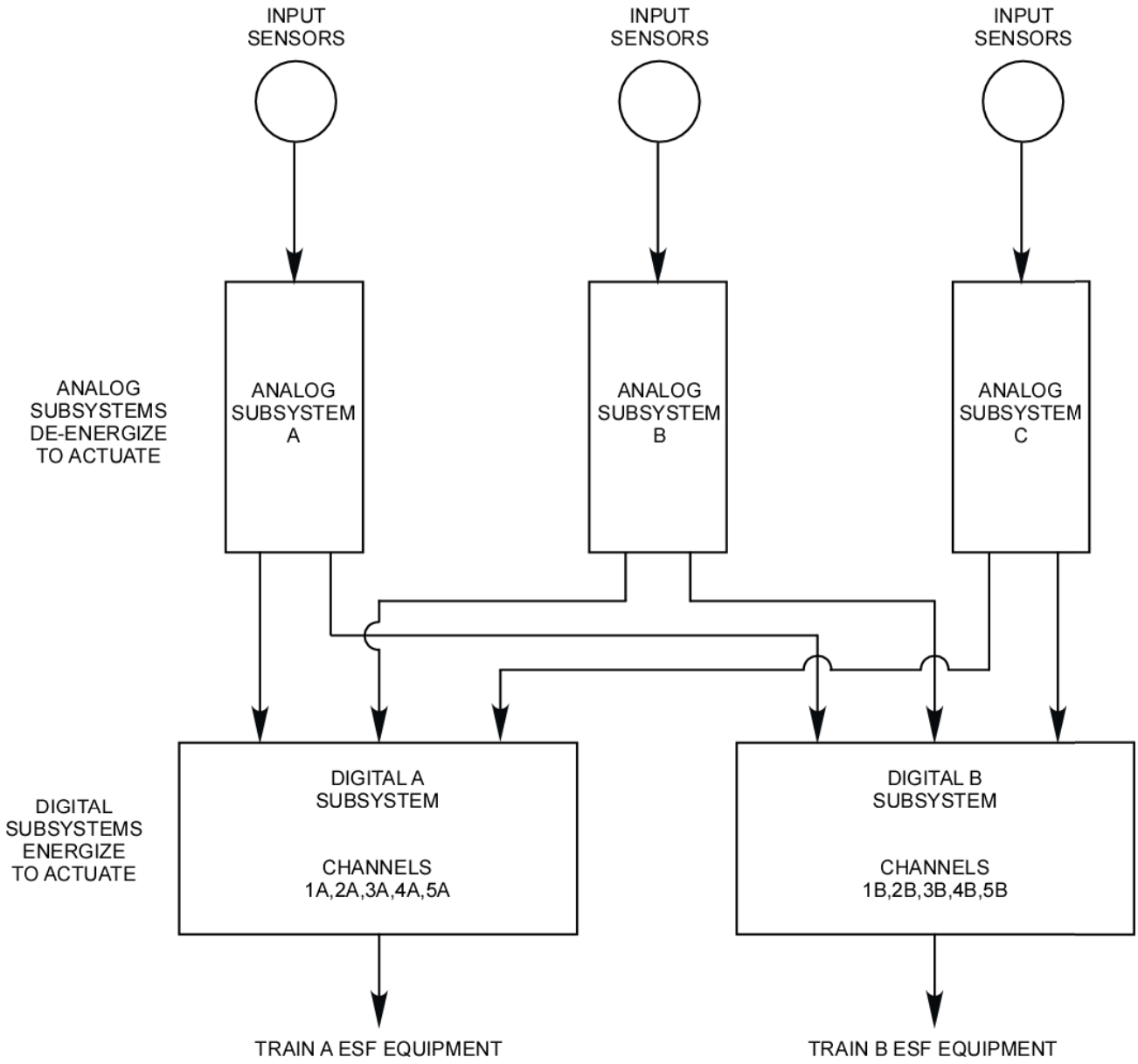
TABLE 10.2-1 ESFAS ACTUATION SUMMARY

Actuation Signals	Digital Channels	Actuated Systems/Components
Low RCS Pressure (<1600 psig) High RB Pressure (>4 psig)	1A, 1B	High Pressure Injection Low Pressure Injection Makeup System Isolation Auxiliary Feedwater Diesel Generators Turbine Trip
Low RCS Pressure (<1600 psig) High RB Pressure (>4 psig)	2A, 2B	All Nonsafety-related RB Penetrations
High-High RB Pressure (>25 psig)	3A, 3B	RB Spray Header Isolation Valves
High-High RB Pressure (>25 psig)	4A, 4B	RB Spray Pumps
Low BWST Level (<5.1 ft)	5A, 5B	LPI Sump Suction Valves RB Spray Sump Suction Valves

TABLE 10.2-2 SECONDARY PROTECTION SYSTEM SUMMARY

CHANNEL A		**CHANNEL B**	
Sub-Channel A1 A-OTSG	Sub-Channel A2 B-OTSG	Sub-Channel B1 A-OTSG	Sub-Channel B2 B-OTSG
Close MSIVs Close MFIV - V17A Start 1A & 3C AFW Trip both MFPs	Close MSIVs Close MFIV - V29A Start 1A & 3C AFW Trip both MFPs	Close MSIVs Close MFIV - V16B Start 2B & 3C AFW Trip both MFPs	Close MSIVs Close MFIV - V28B Start 2B & 3C AFW Trip both MFPs

This page intentionally blank.



CHANNEL	EQUIPMENT
1A, 1B	HPI, LPI, EDGs, AFW, TURBINE TRIP, M/U SYSTEM ISOLATION
2A, 2B	RB ISOLATION AND COOLING
3A, 3B	RB SPRAY ISOLATION VALVES
4A, 4B	RB SPRAY PUMPS
5A, 5B	SUMP RECIRCULATION

Figure 10.2-1 Engineered Safety Features Actuation System (Block Diagram)

This page intentionally blank

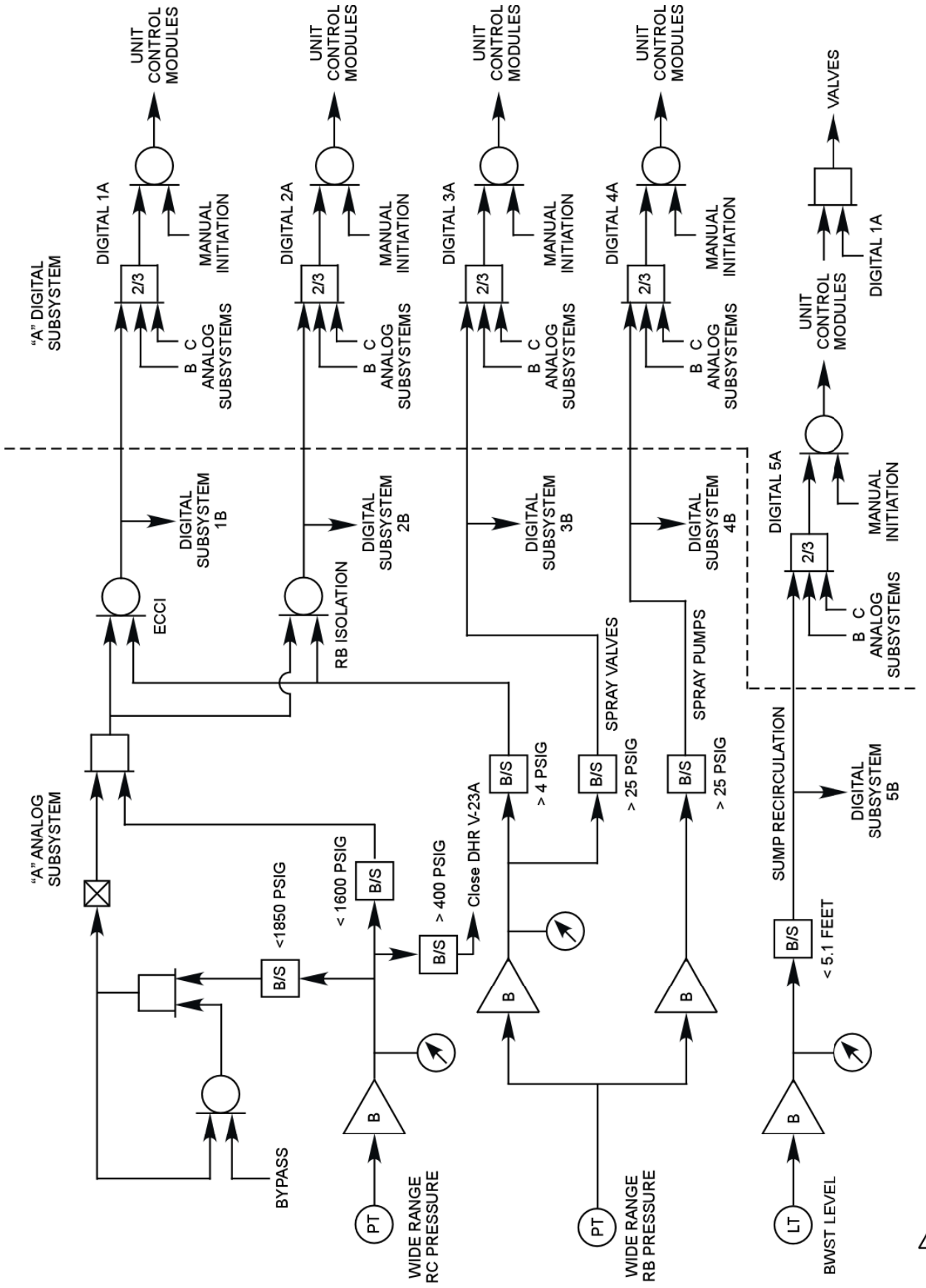


Figure 10.2-2 Engineered Safety Features Actuation System

This page intentionally blank

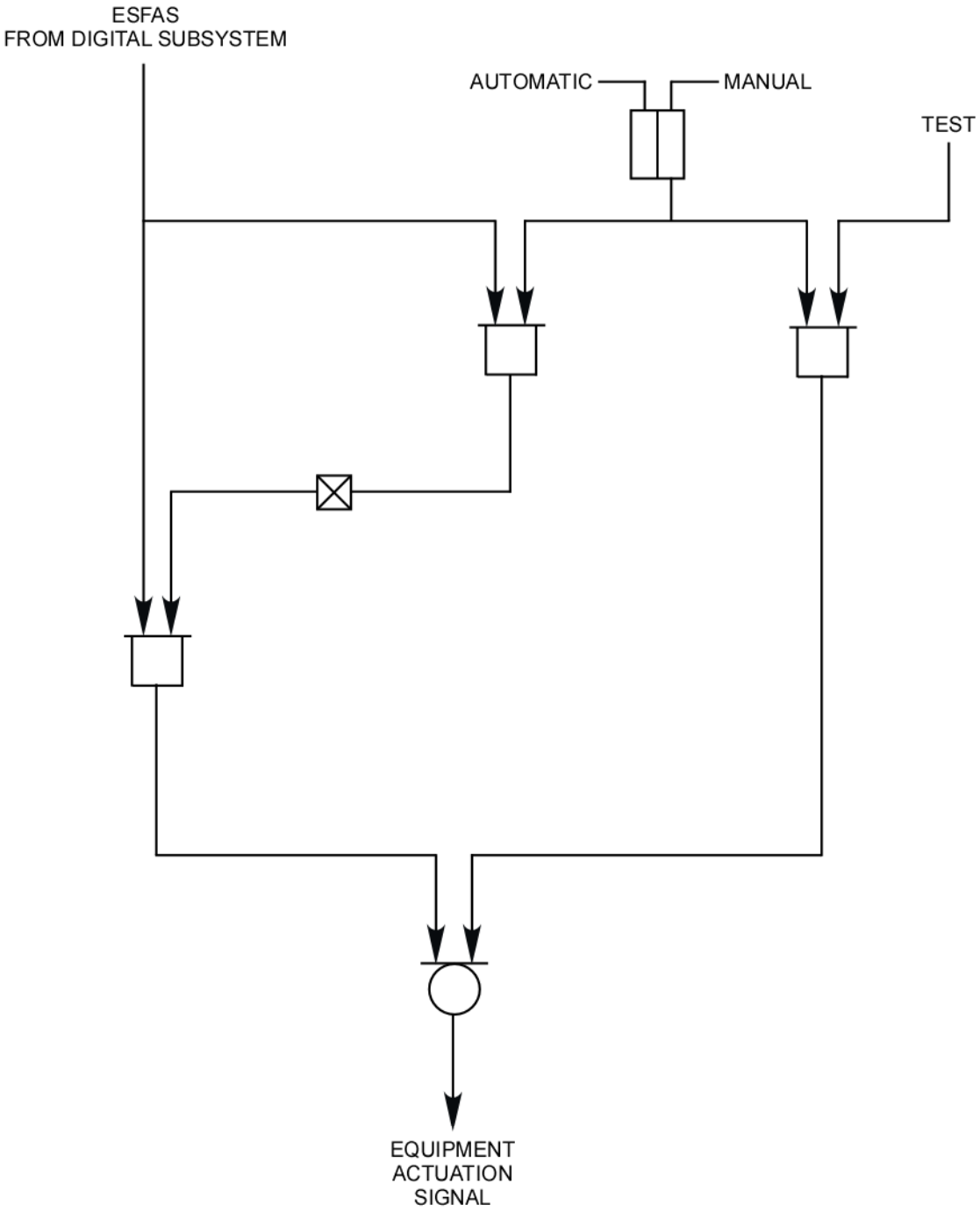


Figure 10.2-3 Unit Control Module Logic

This page intentionally blank

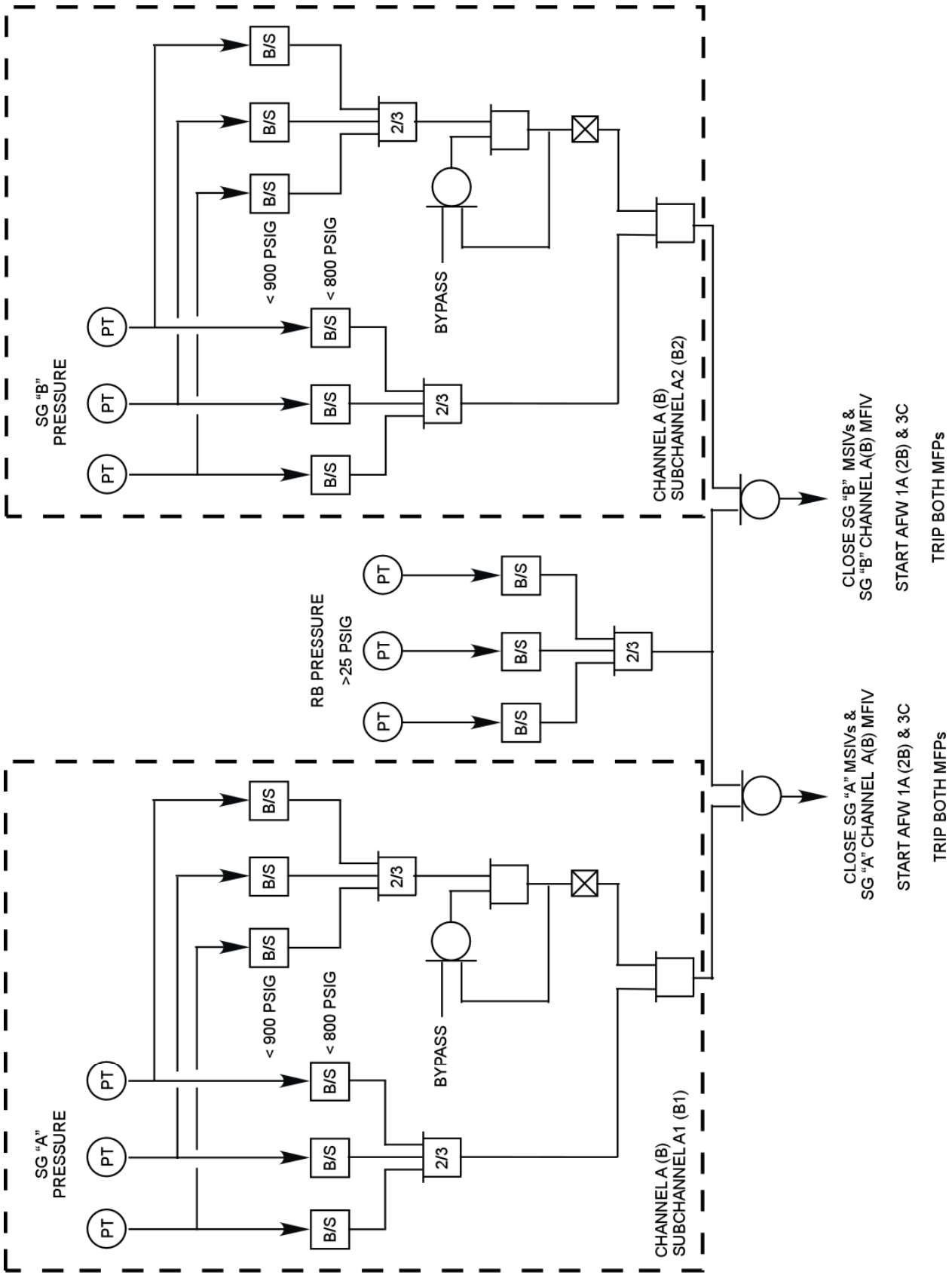


Figure 10.2-4 Secondary Protection System

This page intentionally blank