WESTINGHOUSE CLASS 3 (Non-Proprietary)

Westinghouse Energy Systems

WESTINGHOUSE CLASS 3 (Non-Proprietary)

Westinghouse Energy Systems

WESTINGHOUSE CLASS 3

WCAP-13662

Advanced Passive Plant Protection

System FMEA

Westinghouse Electric Corporation
Energy Systems Business Unit
Nuclear And Advanced Technology Division
P.O. Box 355
Pittsburgh, Pennsylvania 15230

AP600 DOCUMENT COVER SHEET

Form 58202D(5/93) [WPxxxx:1D]
0008 FRM

AP600 DB USE ONLY ____ Pages Attached ____

AP600 DOCUMENT NO.	REVISION NO.	DATED	CONTROLLED COPY NUMBER:
GW-JJ-002	0	April, 1993	ASSIGNED TO:

ALTERNATE DOCUMENT NUMBER: WCAP-13662 (NP)

DESIGN AGENT ORGANIZATION: Westinghouse

PROJECT: AP600

TITLE: Advanced Passive Plant Protection System FMEA

WORK BREAKDOWN #: 2.2.8.2

This section incorporates the following design changes DCP #/Rev.:

ATTACHMENTS

☒ **WESTINGHOUSE PROPRIETARY CLASS 2**

THIS DOCUMENT CONTAINS INFORMATION PROPRIETARY TO WESTINGHOUSE ELECTRIC CORPORATION; IT IS SUBMITTED IN CONFIDENCE AND IS TO BE USED SOLELY FOR THE PURPOSE FOR WHICH IT IS FURNISHED AND RETURNED UPON REQUEST. THIS DOCUMENT AND SUCH INFORMATION IS NOT TO BE REPRODUCED, TRANSMITTED, DISCLOSED OR USED OTHERWISE IN WHOLE OR IN PART WITHOUT PRIOR WRITTEN AUTHORIZATION OF WESTINGHOUSE ELECTRIC CORPORATION, ENERGY SYSTEMS BUSINESS UNIT, SUBJECT TO THE LEGENDS CONTAINED HEREOF.

GOVERNMENT LIMITED RIGHTS:

(A) THESE DATA ARE SUBMITTED WITH LIMITED RIGHTS UNDER GOVERNMENT CONTRACT NO. DE-AC03-90SF18495. THESE DATA MAY BE REPRODUCED AND USED BY THE GOVERNMENT WITH THE EXPRESS LIMITATION THAT THEY WILL NOT, WITHOUT WRITTEN PERMISSION OF THE CONTRACTOR, BE USED FOR PURPOSES OF MANUFACTURER NOR DISCLOSED OUTSIDE THE GOVERNMENT; EXCEPT THAT THE GOVERNMENT MAY DISCLOSE THESE DATA OUTSIDE THE GOVERNMENT FOR THE FOLLOWING PURPOSES, IF ANY, PROVIDED THAT THE GOVERNMENT MAKES SUCH DISCLOSURE SUBJECT TO PROHIBITION AGAINST FURTHER USE AND DISCLOSURE:

(I) THIS "PROPRIETARY DATA" MAY BE DISCLOSED FOR EVALUATION PURPOSES UNDER THE RESTRICTIONS ABOVE.

(II) THE "PROPRIETARY DATA" MAY BE DISCLOSED TO THE ELECTRIC POWER RESEARCH INSTITUTE (EPRI), ELECTRIC UTILITY REPRESENTATIVES AND THEIR DIRECT CONSULTANTS, EXCLUDING DIRECT COMMERCIAL COMPETITORS, AND THE DOE NATIONAL LABORATORIES UNDER THE PROHIBITIONS AND RESTRICTIONS ABOVE.

(B) THIS NOTICE SHALL BE MARKED ON ANY REPRODUCTION OF THESE DATA, IN WHOLE OR IN PART.

□ **WESTINGHOUSE CLASS 3 (NON PROPRIETARY)**

EPRI CONFIDENTIAL/OBLIGATION NOTICES:

NOTICE: 1 □ 2 □ 3 ☒ 4 □ 5 □ CATEGORY: A ☒ B □ C □ D □ E □ F □

☒ **DOE CONTRACT DELIVERABLES (DELIVERED DATA)**

SUBJECT TO SPECIFIED EXCEPTIONS, DISCLOSURE OF THIS DATA IS RESTRICTED UNTIL SEPTEMBER 30, 1995 OR DESIGN CERTIFICATION UNDER DOE CONTRACT DE-AC03-90SF18495, WHICHEVER IS LATER.

ORIGINATOR S. Morandini	SIGNATURE/DATE S. Morandini 4-29-93
AP600 RESPONSIBLE MANAGER B. Reid	B Reid 4/28/93

AP600 STANDARD INTERNAL REVIEW SHEET

Form 58203A (3-91)

AP600 DOCUMENT NO. GW-JJ-002 REVISION 0

ALTERNATE DOC. NO. WCAP-13662

DESIGN AGENT ORGANIZATION Westinghouse

TITLE Advanced Passive Plant Protection System FMEA

WORK BREAKDOWN STRUCTURE NUMBER: 2.2.8.2

W PROPRIETARY CLASS: Class I ____ Class II ____ Class III X

EPRI CONFIDENTIAL/OBLIGATION NOTICES:

NOTICE: 1 □ 2 □ 3 ☒ 4 □ 5 □ CATEGORY: A ☒ B □ C □ D □ E □ F □

REVIEWS	SIGNATURE	DATE	COMMENTS
1. ORIGINATOR S. Morandini	S. Morandini	4-28-93	
2. AP600 RESPONSIBLE MANAGER B. Reid	B Reid	4/28/93	(1) (2)
OTHER REVIEWS			
3. B. McIntyre		4/28/93	
4. N. Liparulo		4/28/93	
5. D. Sharp	D. R. Sharp	4/29/93	
6. R. Bruce	R. A. Bruce	4/28/93	
7. T. Anderson		4/28/93	
8.			
9.			
10.			

(1) Approval indicates that all materials, manufacturing and interface concerns have been addressed.

(2) Approval of the responsible manager signifies that all internal reviews have been obtained and all comments resolved.

* Mandatory Review and Approval

THIS SHEET SHOULD BE MAINTAINED INTERNAL TO THE AP600 PROGRAM

Form 58202C (3/92)

EPRI CONFIDENTIALITY / OBLIGATION NOTICES

NOTICE 1:

The data in this document is subject to no confidentiality obligations.

NOTICE 2:

The data in this document is proprietary and confidential to Westinghouse Electric Corporation and/or its Contractors. It is forwarded to recipient under an obligation of Confidence and Trust for limited purposes only. Any use, disclosure to unauthorized persons, or copying of this document or parts thereof is prohibited except as agreed to in advance by the Electric Power Research Institute (EPRI) and Westinghouse Electric Corporation. Recipient of this data has a duty to inquire of EPRI and/or Westinghouse as to the uses of the information contained herein that are permitted.

NOTICE 3:

The data in this document is proprietary and confidential to Westinghouse Electric Corporation and/or its Contractors. It is forwarded to recipient under an obligation of Confidence and Trust for use only in evaluation tasks specifically authorized by the Electric Power Research institute (EPRI). Any use, disclosure to unauthorized persons, or copying this document or parts thereof is prohibited except as agreed to in advance by EPRI and Westinghouse Electric Corporation. Recipient of this data has a duty to inquire of EPRI and/or Westinghouse as to the uses of the information contained herein that are permitted. This document and any copies or excerpts thereof that may have been generated are to be returned to Westinghouse, directly or through EPRI, when requested to do so.

NOTICE 4:

The data in this document is proprietary and confidential to Westinghouse Electric Corporation and/or its Contractors. It is being revealed in confidence and trust only to Employees of EPRI and to certain contractors of EPRI for limited evaluation tasks authorized by EPRI. Any use, disclosure to unauthorized persons, or copying of this document or parts thereof is prohibited. This Document and any copies or excerpts thereof that may have been generated are to be returned to Westinghouse, directly or through EPRI, when requested to do so.

NOTICE 5:

The data in this document is proprietary and confidential to Westinghouse Electric Corporation and/or its Contractors. Access to this data is given in Confidence and Trust only at Westinghouse facilities for limited evaluation tasks assigned by EPRI. Any use, disclosure to unauthorized persons, or copying of this document or parts thereof is prohibited. Neither this document nor any excerpts therefrom are to be removed from Westinghouse facilities.

EPRI CONFIDENTIALITY / OBLIGATION CATEGORIES

CATEGORY "A" (See Delivered Data)

Consists of CONTRACTOR Foreground Data that is contained in an issued reported.

CATEGORY "B" (See Delivered Data)

Consists of CONTRACTOR Foreground Data that is not contained in an issued report, except for computer programs.

CATEGORY "C"

Consists of CONTRACTOR Background Data except for computer programs.

CATEGORY "D"

Consists of computer programs developed in the course of performing the Work.

CATEGORY "E"

Consists of computer programs developed prior to the Effective Date or after the Effective Date but outside the scope of the Work.

CATEGORY "F"

Consists of administrative plans and administrative reports.

DEFINITIONS

DELIVERED DATA

Consists of documents (e.g. specifications, drawings, reports) which are generated under the DOE contract DE-AC03-90SF18495.

WCAP-13662
Rev 0

Westinghouse Proprietary Class 2 Version exists as WCAP-13594

FMEA of Advanced Passive Plant Protection System

Prepared by:

S.J. Morandini
J.J. Birsa
J.S. Wiesemann
S. Kilim

April 1993

TABLE OF CONTENTS

TABLES

FIGURES

Acronyms and Definitions

ADS:	Automatic Depressurization System
A/D, D/A:	Analog to Digital, Digital to Analog
CMOS:	Complementary Metal Oxide Semiconductors
CRC:	Cyclic Redundancy Check
E^2PROM:	Electrically Erasable Programmable Read Only Memory
EPROM:	Erasable Programmable Read Only Memory
EMI:	Electromagnetic Interference
ESFAC:	Engineered Safety Features Actuation Cabinet
FMEA:	Failure Modes and Effects Analysis
I&C:	Instrumentation and Control
I/O:	Input/Output
IPC:	Integrated Protection Cabinet
MDM:	Multibus Diagnostic Monitor
NISPAC:	Nuclear Instrumentation Signal Processing and Control
PAL:	Programmable Array Logic
PLC:	Protection Logic Cabinet
PLS:	Protection Logic System
PMS:	Protection and Safety Monitoring System
PRA:	Probabilistic Risk Assessment
RAM:	Random Access Memory
RFI:	Radio Frequency Interference
ROM:	Read Only Memory
RTD:	Resistance Temperature Detector

AOK Loop: A series loop through the input/output cards mounted in a cabinet that verifies that the input/output cards are energized.

Board Failure: Failure of the board under consideration, due to out of range readings, open circuit when normally closed, closed circuit when normally open, Random Access Memory (RAM) error, Read Only Memory (ROM) error, multiplexer error, bus interface error, central processing unit (CPU) error, timer error, power supply or interface fault, or input/output error.

Channel Bypass Mode: Disables the individual channel bistable trip function which forces the associated logic to remain in the non-tripped state until the bypass is removed. Used during test operations.

Channel Trip Mode: Interrupts the individual channel bistable outputs to the logic to force the function into a tripped or actuated state.

Fault Tolerance

The ability of an instrumentation and control system to continue design basis operation after the occurrence of a failure within the system.

Partial Actuation:

Actuation demand on one channel, 2/4 channels required for actuation. Partial actuation has no effect on plant operation.

Partial Trip:

Trip demand on one channel, 2/4 channels required for trip. Partial trip has no effect on plant operation.

Self-testing:

Diagnostics which include RAM tests, EPROM/E^2PROM tests, numeric data processing tests, crystal time base checks, calibration checks, CRC checks, and deadman timer checks.

1. Introduction

The purposes of this FMEA are as follows:

- To evaluate the effects of various failure modes on the operational success of the system
- To list potential failures and identify the importance of their effects
- To assist in the objective evaluation of design requirements related to redundancy, failure detection systems, fail-safe characteristics, and automatic and manual override.

This FMEA is consistent with the guidance presented in ANSI/IEEE Std 352 and associated documents, as shown in section 8 of this document.

2. Methods

The guidance given in References 2 and 3 is followed. The single failure criterion is applied to this analysis.

Results show that single failures of the PMS have no effect on plant operation. Certain unlikely failures in the logic cabinets can initiate end device actuation (nuisance failures). These actuations constitute the single component failure criterion included in the fluid systems design basis. See section 4.6 of this document for a discussion of nuisance failures.

3. Description of System to be Analyzed and its Mission

The Protection and Monitoring System (PMS) performs the following functions:

- determines if plant safety limits have been exceeded
- automatically trips the reactor
- actuates engineered safeguards equipment
- provides safety grade plant monitoring, prior to, during, and after an accident or plant transient

The protection and safety monitoring system architecture is shown in Figure 1. In this architecture, related functions are grouped into cabinets. Cabinets are then connected into systems by means of hard wired conductors, datalinks, and data highways. The cabinets also communicate between systems through a plant wide highway termed the Monitor Bus.

The I&C architecture is arranged in a hierarchical manner. Below the Monitor Bus are the systems and functions that perform the protective, control, and data monitoring functions.

This analysis examines the Protection and Safety Monitoring System (PMS). Included in the PMS are the Integrated Protection Cabinets, the Engineered Safety Features Actuation Cabinets, and the Protection Logic Cabinets. The Protection and Safety Monitoring System provides actuating signals to the reactor trip breakers and to the Engineered Safety Features equipment in the event of an accident.

The Integrated Protection Cabinets contain the reactor trip subsystem, the trip enable subsystem, the global trip subsystem, the dynamic trip bus, the engineered safety features subsystem and communications subsystem. These cabinets, their related sensors and reactor trip switchgear, are four-way redundant.

The Engineered Safety Features Actuation Cabinets (ESFACs) perform system-level logic calculations such as initiation of Safety Injection. They receive inputs from the Integrated Protection Cabinets and the control room.

The Protection Logic Cabinets provide the capability for on-off control of individual plant loads for Class 1E applications. They receive inputs from the ESFACs and the control room via the Main Control Room Multiplexers.

The Protection and Safety Monitoring System provides four instrumentation channels and outputs to four actuation or trip logic trains for each protective function. An exception to this are the start-up feedwater functions which have two instrumentation channels, and employ 1/2 logic. Reactor trip functions and Engineered Safety Features Actuation functions, with the exception of the startup feedwater functions, have four independent channels (sensors). Where four channels are provided, a 2/4 logic with bypass is provided so that a channel may be taken out of service (or fail) without any loss of protective function. Redundant channels and trains are electrically isolated and physically separated.

Electrical power for the Protection and Safety Monitoring System instrumentation is obtained from four separate uninterruptable instrument buses. The use and availability of the four buses is related to the Protection and Safety Monitoring System instrumentation in the following ways:

- Each of the four instrument buses is assigned to one of the safety divisions.

- The design of the I&C will prevent the loss of a single bus from putting the plant in an unprotected condition.

- Upon loss of power, the solid state switches in the Instrumentation and Control Cabinets transfer to a nonconducting or open circuit state. In other words, all Instrumentation and Control Cabinet outputs will deenergize.

- Instrument channels are arranged so that loss of any one bus will not force a reactor trip. (e.g. the 2/4 reactor trip logic will revert immediately to a 1/3 trip logic.)

- Coincident loss of any two buses will trip the reactor immediately.

Table 1 lists the boards of the protection system which are considered in this FMEA, and the location of each board. The protection system is described in detail in Reference 1.

4. Analysis Boundaries and Failure Modes

This FMEA examines the components required to perform the functions listed above. The lowest level of line replaceable units, circuit boards, is analyzed. Not included are the final actuated devices. The FMEA is documented in Table 2. The circuit boards which are discussed below are analyzed. Common mode failures are not addressed here, but are evaluated in Reference 4.

Due to the failure detection provided by self-testing and redundancy, most single circuit board failures are detectable. A small portion of failures for selected boards could be undetectable, but only if they were to occur in the brief time between self tests. This failure mode was examined and concluded to be an inconsequential failure contributor due to the small portion of failures of this type with respect to the total possible board failures, and due to the limited time window between self tests. Because of the small chance of undetectable failures, this analysis examines only the detectable failures, such as those which overtly cause loss of function.

4.1 Microprocessor chassis:

4.1.1 Functional processor (M12)

The functional processor performs the major computations required to achieve the specific function of the microprocessor chassis subsystem in which it has been installed. Tasks performed by the functional processor include: movement of data between subsystem memories or I/O registers for input or output, on-line compensation of analog inputs, conversion of input data to engineering units, computations, and diagnostic testing. Parity-checking of RAM is used to detect corruption of data. An onboard numeric data co-processor is used in subsystems that perform floating point arithmetic. The functional processor also has a serial port to accommodate a maintenance terminal that is used for off-line diagnostics. A functional processor is included in all subsystems as the subsystem host processor, except where a logic processor is provided.

[

]$^{(a,c)}$

Colored LEDs (Light Emitting Diodes) are available on the functional processor to provide indication of the processor's operational status.

The M12 board is present in many different applications:

- Integrated protection cabinets (IPCs)
  - Engineered safety features subsystem
  - Reactor trip subsystems
  - Global trip subsystem
  - Trip enable subsystem
  - Nuclear instrumentation signal processing and control (NISPAC) subsystem
- Engineered safety features actuation cabinets (ESFAC) subsystems
- Protection logic cabinets

Figures 2 - 8 show the subsystems present in the protection system.

Failure modes for the M12 include the following:

- Failure to compute
- Failure to read
- Failure to write
- Failure to store
- Failure to address
- Failure of interrupts

These can be summarized as:

- Functional failures: Failures which corrupt normal sequential processing of main code.
- Data failures: Failures which do not inhibit the main processing, but alter the input and output data which is needed and produced by the main code.
- CMOS and PAL logic failures: Those failures involving Complementary Metal-Oxide Semiconductors (CMOS) and other MOS family devices, as well as Programmable Array Logic (PAL) devices, which can potentially fail logically, giving unexpected input/output characteristics, rather than at a classical stuck-at high or low failure state.

Possible effects of these failures for IPC usage are inadvertent partial trip, inadvertent partial actuation, partial trip failure, or partial actuation failure. These will have no effect on plant operations due to the 2/4 logic and the presence of the three remaining redundant channels. For ESFAC applications, a single detectable failure would have no effect due to fault tolerance in the logic cabinet design, accomplished by means of failure detection and corrective actions such as bypass of the channel. Redundant design allows the three remaining channels to continue operation. A small portion of ESFAC failures could be undetectable during the brief time window between self-test cycles. During this time, a failure of the false good health status type or erroneous signal generation could result.

4.1.2 Logic processor (M03)

The logic processor is provided in Protection Logic Cabinets to perform logic calculations on the input signals acquired by the Logic Bus data highway controller or a local I/O board and to generate logic outputs to be sent to the power interface I/O boards. There are four logic processors in each Protection Logic Cabinet. Two logic processors reside in each of two functional logic subsystems. Logic processors serve as the subsystem host processors in each functional logic subsystems.

The logic processor performs the computations required to achieve the specific function of the microprocessor chassis subsystem in which it has been installed. Tasks performed by the logic processor include: movement of data between subsystem memories or I/O registers for input or output, computations, and diagnostic testing. Parity-checked RAM is used to detect corruption of data. [

]$^{(a,c)}$

The M03 is similar to the functional processor, but is used where no floating point or math coprocessor is required, such as in the logic cabinets. A single M03 failure would have no effect on plant operation, due to fault tolerance in the logic cabinet design. This is accomplished by means of failure detection and corrective actions such as bypass of the failed channel. Redundant design allows the three remaining channels to continue operation.

4.1.3 Data highway controller (M51)

The data highway controller is a microprocessor based board that provides the interface between a subsystem host processor and a data highway transceiver (I/O) board. The data highway controller receives outgoing data from the processor board in on-board shared memory via the IEEE STD 796 bus, performs the necessary formatting and conversions on this data, and transfers this data to a local (on-board) communications controller which transmits the data to the transceiver board. Incoming data is received from the transceiver board by the local communications controller, interpreted and converted, and placed in the on-board shared memory, where it is accessed by the subsystem host processor board via the IEEE STD 796 bus.

[

]$^{(a,c)}$

Failure modes for the data highway controller include data transmission errors, and bus errors. Single failures have no effect due to fault tolerance in logic cabinet design. This is accomplished by means of failure detection and corrective actions such as bypass of the failed channel. Redundant design allows the three remaining channels to continue operation.

4.1.4 Parallel input/output (I/O) board (M19)

The handling of individual logic signals, such as contact inputs and light outputs, in a microprocessor chassis subsystem is accomplished by means a parallel input/output board. Output data is transferred from the subsystem host processor to I/O registers on this board, then from these registers to output ports. Inputs are sampled at input ports and stored in I/O registers on the board to be accessed by the subsystem host processor. [

]$^{(a,c)}$

[

]$^{(a,c)}$

Failure of this board can result in a bus failure, and can result in a partial trip or partial actuation, depending on the microprocessor subsystem in which the board is used. For instance, failure of a board used in a subsystem whose function is to generate a reactor trip can cause a partial trip, but not a partial ESF actuation. Conversely, failure of a board used in an ESF actuation subsystem but not a reactor trip subsysten will generate partial ESF actuation. Table 1 shows board application details.

4.1.5 Isolated parallel I/O board (M56)

In the few instances where subsystem to subsystem I/O is required, optical coupled I/O is utilized on the isolated parallel I/O board. Other than this board having fewer I/O lines and the input lines being provided with optical isolation, this board functions identically to the parallel I/O board (M19). Output data is transferred from the subsystem host processor to I/O registers on this board, then from these registers to output ports. Optically isolated inputs are sampled at input ports and stored in I/O registers on the board to be accessed by the subsystem host processor.

[

]$^{(a,c)}$

Failure of this board can cause a bus failure, and can result in a partial trip or partial actuation, depending on the microprocessor subsystem in which the board is used. For instance, failure of a boaru used in a subsystem whose function is to generate a reactor trip can cause a partial trip, but not a partial ESF actuation. Conversely, failure of a board used in an ESF actuation subsystem bu not a reactor trip subsystem will generate partial ESF actuation. Table 1 shows board application details.

4.1.6 Analog input processor (M40)

The Analog Input Processor is a microprocessor based I/O board that converts analog input signals to digital data and performs digital signal conditioning (i.e. averaging, filtering algorithms, etc.) on this digital data. The filtered digital data is then placed in shared memory for access by the subsystem host processor via the IEEE Std. 796 bus. Each analog input processor supports up to eight differential analog input channels. The analog input processor performs analog to digital conversion, signal status checks, input calibration readings and onboard diagnostics. Filtered input data is provided to the subsystem host processor for calibration calculations. [

]$^{(a,c)}$

[

]$^{(a,c)}$

Failure of this board can cause a partial trip or partial actuation, depending on the microprocessor subsystem in which the board is used. For instance, failure of a board used in a subsystem whose function is to generate a reactor trip can cause a partial trip, but not a partial ESF actuation. Conversely, failure of a board used in an ESF actuation subsystem but not a reactor trip subsystem will generate partial ESF actuation. Table 1 shows board application details.

4.1.[illegible] Universal memory expansion board (M28)

A general purpose memory board is used in instances where the subsystem host processor does not possess sufficient memory to perform its required functions. Access to the memory is via the IEEE STD-796 bus and is functionally identical to the subsystem host processor onboard memory. [

]$^{(a,c)}$

Possible effects of M28 failures for IPC usage are inadvertent partial trip, inadvertent partial actuation, partial trip failure, or partial actuation failure. These have no effect on plant operations due to the 2/4 logic and the presence of the three remaining redundant channels. For ESFAC applications, a single detectable failure would have no effect due to fault tolerance in the logic cabinet design, accomplished by means of failure detection and corrective actions such as bypass of the failed channel. Redundant design allows the three remaining channels to continue operation. A small portion of ESFAC failures could be undetectable during the brief time window between self-test cycles. During this time, a failure of the false good health status type or erroneous signal generation could result.

4.1.8 Serial Communications Controller (M48)

This board provides multiple serial data link communication functions for subsystem host processors. It is used to provide communications within cabinet sets between the various subsystems and also with the portable test/maintenance station.

[

]$^{(a,c)}$

For IPC applications, the effect M48 board failures can be a partial trip or partial actuation, depending on board usage. For ESFAC applications, single failures have no effect due to fault tolerance in logic cabinet design, accomplished by means of failure detection and corrective actions such as bypass of the failed channel. Redundant design allows the three remaining channels to continue operation.

4.2 Termination frame assembly

4.2.1 Analog input board (EAI)

The analog input board provides an interface between field sensors and an associated analog input processor (M40 analog to digital conversion board). Each analog input board provides [ ]$^{(a,c)}$ analog input buffer/translator channels and [ ]$^{(a,c)}$ isolated loop power supplies. [

]$^{(a,c)}$ sensor inputs.

[

]$^{(a,c)}$

The analog input board is mounted in a slot in the termination frame at the rear of an instrument cabinet. The analog input board provides IEEE STD-472-1974 Surge Withstand Capability and overvoltage protection for all field conductors. The board is keyed to prevent the insertion of an incorrect board in a termination frame.

Failure of this board can cause a partial trip or partial actuation, depending on the subsystem in which the board is used. For instance, failure of a board used in a subsystem whose function is to generate a reactor trip can cause a partial trip, but not a partial ESF actuation. Conversely, failure of a board used in an ESF actuation subsystem but not a reactor trip subsystem will generate partial ESF actuation. Table 1 shows board application details.

4.2.2 RTD Input Board (ERI)

The RTD input board provides an interface between 4-wire RTD's (Resistance Temperature Detectors) and an associated analog input processor (M40 analog to digital conversion board). Each RTD input board provides [ ]$^{(a,c)}$ analog input buffer/translator channels and [ ]$^{(a,c)}$ isolated RTD power supplies. [

]$^{(a,c)}$

[

]$^{(a,c)}$

The RTD input board is mounted in a slot in the termination frame at the rear of an instrument cabinet. The RTD input board provides IEEE STD-472-1974 Surge Withstand Capability and overvoltage protection for all field conductors. The board is keyed to prevent the insertion of an incorrect board in a termination frame.

Failure of this board can cause a partial trip or partial actuation, depending on the subsystem in which the board is used. For instance, failure of a board used in a subsystem whose function is to generate a reactor trip can cause a partial trip, but not a partial ESF actuation. Conversely, failure of a board used in an ESF actuation subsystem but not a reactor trip subsystem will generate partial ESF actuation. Table 1 shows board application details.

4.2.3 Digital (Contact) Input Board (ECI)

The digital input board provides an interface between field contacts and an associated parallel I/O board (M19 digital input/output board). Each digital input board provides [ ]$^{(a,c)}$ digital input channels, capable of handling a combination of up to [ ]$^{(a,c)}$ Each digital input channel provides an independent contact wetting power supply at 48 VDC, contact debounce and filtering, signal conversion, signal injection for autotest, and electrical isolation functions for the field inputs.

[

]$^{(a,c)}$

The digital input board is mounted in a slot in the termination frame at the rear of an instrument cabinet. The digital input board provides IEEE STD-472-1974 Surge Withstand Capability and overvoltage protection for all field conductors. The board is keyed to prevent the insertion of an incorrect board in a termination frame.

Failure of this board can cause a partial trip or partial actuation, depending on the subsystem in which the board is used. For instance, failure of a board used in a subsystem whose function is to generate a reactor trip can cause a partial trip, but not a partial ESF actuation. Conversely, failure of a board used in an ESF actuation subsystem but not a reactor trip subsystem will generate partial ESF actuation. Table 1 shows board application details.

4.2.4 Digital (Contact) Output Board (ECO)

The digital output board provides the necessary signal translation for a parallel I/O board (M19 digital input/output board) in a microprocessor chassis subsystem to drive loads external to the instrumentation cabinet. Each digital output board provides [

]$^{(a,c)}$ relay contact output. The digital output board also contains a deadman timer to disable output transition upon failure of the associated parallel I/O board.

The digital output board is mounted in a slot in the termination frame at the rear of an instrument cabinet. The digital output board provides IEEE STD-472-1974 Surge Withstand Capability and overvoltage protection for all field conductors. The digital output board provides Class 1E isolation for its [ ]$^{(a,c)}$ output channels. The board is keyed to prevent the insertion of an incorrect board in a termination frame.

Failure of this board can cause a partial trip.

4.2.5 Reactor Coolant Pump Speed Sensor Input Board (ESI)

The reactor coolant pump speed sensor input board provides the interface for the magnetic speed sensor mounted on a reactor coolant pump. [

]$^{(a,c)}$

[

]$^{(a,c)}$

The reactor coolant pump speed sensor input board is mounted in a slot in the termination frame at the rear of an instrument cabinet. The reactor coolant pump speed sensor input board provides IEEE STD-472-1974 Surge Withstand Capability and overvoltage protection for all field conductors. The board is keyed to prevent the insertion of an incorrect board in a termination frame.

Failure of this board can cause a partial trip.

4.2.6 Power Interface (2/3 Voted) Output Board (EPO)

The power interface output board provides an interface between field loads, field contacts, and [ ]$^{(a,c)}$ logic processors (M03) via each logic processor's I/O bus controller daughterboard. Each power interface output board provides [ ]$^{(a,c)}$ contact outputs to drive plant loads. Each power interface output board also provides a group of [ ]$^{(a,c)}$ digital input channels, each channel capable of handling a [ ]$^{(a,c)}$ contact input. [ ]$^{(a,c)}$ There are [ ]$^{(a,c)}$ independent microprocessors on the power interface output board that drive the output contacts through a 2/3 voting circuit. The microprocessors also sense the input contact positions and each transmits the data on its respective I/O bus.

[ ]$^{(a,c)}$

The power interface output board provides a fast shutoff option that interrupts power to the load when certain input contacts close. This is intended to directly stop movement of a motor operated valve when the torque switch actuates without a command being required from the logic processors.

The power interface output board is mounted in a slot in the termination frame at the rear of an instrument cabinet. The digital input board provides IEEE STD-472-1974 Surge Withstand Capability for all field conductors. The board is keyed to prevent the insertion of an incorrect board in a termination frame.

Failure of this board can cause inadvertent actuation or actuation failure of end device.

4.2.7 Power Interface Relay Driver Board (EPR)

The power interface relay driver board provides an interface between field loads and [ ]$^{(a,c)}$ logic processors (M03) via each logic processor's I/O bus controller daughterboard. Each power interface relay driver board provides [ ]$^{(a,c)}$ contact outputs to drive plant loads. There are [ ]$^{(a,c)}$ independent microprocessors on the power interface relay driver board that drive the output contacts through a 2/3 voting circuit.

[

]$^{(a,c)}$

The power interface relay driver board is mounted in a slot in the termination frame at the rear of an instrument cabinet. The digital input board provides IEEE STD-472-1974 Surge Withstand Capability for all field conductors. The board is keyed to prevent the insertion of an incorrect board in a termination frame.

Failure of this board can cause inadvertent actuation or actuation failure of end device.

4.2.8 Power Interface (Contact) Input Board (EPI)

The power interface input board provides an interface between field contacts and [ ]$^{(a,c)}$ logic processors (M03) via each logic processor's I/O bus controller daughterboard. Each power interface input board provides [ ]$^{(a,c)}$ digital input channels, each channel capable of handling a [ ]$^{(a,c)}$ contact input. Each group of channels is provided with an independent contact wetting power supply at 48 VDC. [

]$^{(a,c)}$. There are [ ]$^{(a,c)}$ independent microprocessors on the power interface input board that sense the contact positions and each transmits the data on its respective I/O bus.

The power interface input board is mounted in a slot in the termination frame at the rear of an instrument cabinet. The digital input board provides IEEE STD-472-1974 Surge Withstand Capability for all field conductors. The board is keyed to prevent the insertion of an incorrect board in a termination frame.

Failure of this board can cause inadvertent actuation or actuation failure of end device.

4.2.9 Optical Datalink Transmitter Board (ETX)

The optical datalink transmitter board provides interface capability between serial communications controllers (M48) in a microprocessor chassis subsystem and external instrumentation cabinets or systems over optical datalink media. The optical datalink transceiver board provides [ ]$^{(a,c)}$ optical datalink output channels for communications to external instrumentation cabinets. The optical datalink transmitter board has [ ]$^{(a,c)}$ internal datalink channels for communications inside the instrumentation cabinet. The optical datalink transmitter board performs the required signal translation between the internal and external communications channels.

[

]$^{(a,c)}$

The optical datalink transmitter board is mounted in a slot in the termination frame at the rear of an instrument cabinet. The board is keyed to prevent the insertion of an incorrect board in a termination frame.

Failure of this board or interconnecting fiber optic lines can cause a partial trip or partial actuation, depending on the subsystem in which the board is used. For instance, failure of a board used in a subsystem whose function is to generate a reactor trip can cause a partial trip, but not a partial ESF actuation. Conversely, failure of a board used in an ESF actuation subsystem but not a reactor trip subsystem will generate partial ESF actuation. Table 1 shows board application details.

4.2.10 Optical Datalink Receiver Board (ERX)

The optical datalink receiver board provides interface capab:lity between serial communications controllers (M48) in a microprocessor chassis subsystem and external instrumentation cabinets or systems over optical datalink media. The optical datalink transceiver board provides [ ]$^{(a,c)}$ optical datalink input channels for communications to external instrumentation cabinets. The optical datalink receiver board has [ ]$^{(a,c)}$ internal datalink channels for communications inside the instrumentation cabinet. [ ]$^{(a,c)}$. The optical datalink receiver board performs the required signal translation between the internal and external communications channels.

[ ]$^{(a,c)}$

The optical datalink receiver board is mounted in a slot in the termination frame at the rear of an instrument cabinet. The board is keyed to prevent the insertion of an incorrect board in a termination frame.

Single failures of this board, or interconnecting fiber optic lines, can cause a partial trip for IPC usage. Single failures of this board, or interconnecting fiber optic lines, for ESFAC usage will have no effect due to failure detection and 2/4 logic in the ESFAC.

4.2.11 Data Highway Transceiver Board (EHX)

The data highway transceiver board provides an interface between up to [ ]$^{(a,c)}$ data highway controllers (M51) residing in a microprocessor chassis subsystem and an external data highway. The external data highway can be either a fiber optic data highway, an electrical data highway, or both. The data highway transceiver board performs the required signal translation between the internal and external communications channels. The data highway transceiver board acts as a repeater between the active internal and external communications channels; an incoming message on any channel is retransmitted on all the remaining configured channels.

The data highway transceiver board is mounted in a slot in the termination frame at the rear of an instrument cabinet. The board is keyed to prevent the insertion of an incorrect board in a termination frame.

Single failures of this board have no effect due to fault tolerance in the logic cabinet design. This is accomplished by means of failure detection and corrective actions such as bypass of the failed channel. Redundant design allows the three remairing channels to continue operation.

4.2.12 I/O Bus Extender Board (EBE)

[

]$^{(a,c)}$

[

]$^{(a,c)}$

Failure of thıs board can cause inadvertent actuation or actuation failure of end devices.

4.2.13 I/O Bus Selector Board (XTS)

[

]$^{(a,c)}$

Single failures of this board have no effect due to fault tolerance in logic cabinet design. This is accomplished by means of failure detection and corrective actions such as bypass of the failed channel. Redundant design allows the three remaining cl annels to continue operation.

4.3 Dynamic trip bus

The dynamic trip bus is a specialized assembly used in the Integrated Protection Cabinets that performs the final combinational logic that implements the reactor trip function. This assembly is composed of a backplane on which are mounted two specialized circuit boards, and a special output board. [

]$^{(a,c)}$ The dynamic trip bus assembly contains control switches and indicators to support operator interaction functions, therefore, it is located at the level of operator interaction panels in the cabinet.

[

]$^{(a,c)}$

4.3.1 Dynamic Trip Bus Clock Unit Board (DCU)

[

]$^{(a,c)}$

Failure of this board can cause a partial trip.

4.3.2 Dynamic Trip Bus Logic Unit (DLU)

The dynamic trip bus logic unit (DLU) circuit board contains the building blocks, dynamic logic unit circuits, that implement the combinational logic used for the dynamic trip bus function. [

]$^{(a,c)}$

[

]$^{(a,c)}$

[

]$^{(a,c)}$

Failure of this board can cause a partial trip.

4.3.3 Power Converter Board (EPC)

The power converter board is the last stage of the dynamic trip bus. [

]$^{(a,c)}$

The power converter board is mounted in a slot in the termination frame at the rear of an instrument cabinet. The board is keyed to prevent the insertion of an incorrect board in a termination frame.

Failure of this board can cause a partial trip.

4.4 Nuclear instrumentation input modules (NIMOD)

The Nuclear Instrumentation signal conditioning circuitry is provided in the form of power supply and amplifier modules that are located in a chassis in the Integrated Protection Cabinets, and preamplifiers located external to the cabinets, close to the detectors. Because three types of detectors are required for the entire range of nuclear flux to be monitored, there are also three configurations for the nuclear instrumentation signal conditioning.

Keying is used for all modules and circuit boards to prevent insertion of the wrong module or circuit board into a slot.

4.4.1 Source Range Configuration

The lowest of the three ranges of nuclear instrumentation channels is the source range, which measures thermal neutron flux in the range of [ ]$^{(a,c)}$ and is used during plant shutdowns, refueling, and startups.

[

]$^{(a,c)}$

Failure modes for one channel of the source range instrumentation could cause incorrect signals to be generated, and a partial trip could be initiated.

4.4.2 Intermediate Range Configuration

The next of the three ranges of nuclear instrumentation channels is the intermediate range, which measures thermal neutron flux in the range of [ ]$^{(a,c)}$ and is used during plant shutdowns, and startups to overlap the source and power ranges.

[

]$^{(a,c)}$

Failure modes for one channel of the intermediate range instrumentation could cause incorrect signals to be generated, and a partial trip could be initiated.

4.4.3 Power Range Configuration

The highest of the three ranges of nuclear instrumentation channels is the power range, which measures thermal neutron flux in the range of [ ]$^{(a,c)}$ and is used during plant power operation.

[ ]$^{(a,c)}$

Failure modes for one channel of the power range instrumentation could cause incorrect signals to be generated, and a partial trip could be initiated.

4.4.4 High Voltage Power Supply (DNH)

The high voltage power supply is one of three modules that comprise a Nuclear Instrumentation Module (NIMOD). The high voltage power supply provides the necessary voltage and current to operate the nuclear detectors in a channel.

The high voltage power supply is provided with three different output voltage configurations in order to power the three types of nuclear detectors used for the source range, intermediate range, and power range channels. The high voltage power supply's AC power connector is electrically keyed to prevent installation of an incorrect high voltage power supply in a NIMOD. Short circuit protection and current limiting is provided for all types.

Failure modes for the high voltage power supply could cause signal failure or a wrong output to be generated, resulting in a partial trip.

4.4.5 Low Voltage Power Supply (DNL)

The low voltage power supply (DNL) is one of three modules used to comprise a Nuclear Instrumentation Module (NIMOD). The low voltage power supply provides the necessary voltage to operate the electronic assemblies in a NIMOD. [

]$^{(a,c)}$

Failure modes for the low voltage power supply could cause signal failure or a wrong output to be generated, resulting in a partial trip.

4.4.6 Nuclear Instrumentation Amplifier Modules (DNI)

Each amplifier module consists of an input board and an interface board mounted in a DNI module, together these form an amplifier module appropriate to the type of detector used for the channel. The input boards in the DNI modules provide the necessary low level signal conditioning circuits required by the [ ]$^{(a,c)}$ detectors in the Nuclear Instrumentation Channels. The interface boards provide the necessary interfaces between the input cards and the standard microprocessor system cards (NISPAC) used for signal conversion and processing.

Failure modes for the nuclear instrumentation amplifier module could cause signal failure or a wrong output to be generated, resulting in a partial trip.

4.4.6.1 Source Range Input Board

The source range input board amplifies, conditions, and isolates the signal from the source range detector as part of its function of inputting this signal into the Integrated Protection Cabinets. The source range input board provides input attenuation and amplification, pulse discrimination, buffering, and shaping, test circuitry interfaces, and output isolation to the audio count rate amplifier.

[

]$^{(a,c)}$

[

]$^{(a,c)}$

Failure of the source range input board could cause a partial trip.

4.4.6.2 Source Range Interface Board

The source range interface board contains the interface and isolation circuits required by the source range NIMOD to communicate with the NISPAC computer. The source range interface board provides multiplexing and buffering of analog signals and optical isolation of digital signals for the NISPAC computers, and buffering and conditioning of analog test signals and optical isolation of digital control lines for the automatic tester interface. [

]$^{(a,c)}$

Failure of the source range interface board could cause a partial trip.

4.4.6.3 Intermediate Range Input Board

The intermediate range input board amplifies, conditions, and isolates the signal from the intermediate range detector as part of its function of inputting this signal into the Integrated Protection Cabinets. The intermediate range input board provides variable gain input amplification and test circuitry interfaces.

[

]$^{(a,c)}$

Failure of the intermediate range input board could cause a partial trip.

4.4.6.4 Intermediate Range Interface Board

The intermediate range interface board contains the interface and isolation circuits required by the intermediate range NIMOD to communicate with the NISPAC computer. The intermediate range interface board provides multiplexing and buffering of analog signals and optical isolation of digital signals for the NISPAC computers, and buffering and conditioning of analog test signals and optical isolation of digital control lines for the automatic tester interface.

[

]$^{(a,c)}$

Failure of the intermediate range interface board could cause a partial trip.

4.4.6.5 Power Range Input Board

The power range input board amplifies, conditions, and isolates the signals from the power range detectors as part of its function of inputting these signals into the Integrated Protection Cabinets. The power range input boards provide [ ]$^{(a,c)}$ channels each of current to voltage amplifiers for four separate input channels.

[

]$^{(a,c)}$

Failure of the power range input board could cause a partial trip.

4.4.6.6 Power Range Interface Board

The power range interface board contains the interface and isolation circuits required by the power range NIMOD to communicate with the NISPAC computer. The power range interface board provides multiplexing and buffering of analog signals and optical isolation of digital signals for the NISPAC computers, and buffering and conditioning of analog test signals and optical isolation of digital control lines for the automatic tester interface.

[

]$^{(a,c)}$.

Failure of the power range interface board could cause a partial trip.

4.4.7 Source Range Preamplifier (AAS)

The source range preamplifier (AAS) amplifies the [ ]$^{(a,c)}$ pulses produced by the source range detector and transmits these to the source range amplifier in the Integrated Protection Cabinets. This enables the signal conditioning electronics for the source range detector to be located in the Integrated Protection Cabinets.

[

]$^{(a,c)}$

[

]$^{(a,c)}$

Failure of the source range preamplifier could cause a partial trip.

4.5 Other cabinet modules

4.5.1 DC power supply chassis (ACP)

The DC power supply chassis is a standard dual power supply module that is used to provide combinations of voltages to drive IEEE STD 796 boards, I/O boards, or both. Each DC power supply chassis contains [ ]$^{(a,c)}$ switching power supply units, and [ ]$^{(a,c)}$ switches and potentiometers, mounted on the front panel, for separate on/off control and output voltage adjustment. Up to three DC power supply chassis can be mounted in an instrument cabinet.

[

]$^{(a,c)}$

Power and signal connections are made by means of modular connectors at the rear of the DC power supply chassis. These connectors are assembled and keyed in such a fashion that only an identical unit, with the same input and output configuration, can be connected in place of a removed unit.

Each of the two power supplies mounted in the DC power supply chassis is provided with an on/off switch on the front panel. Each of the voltage outputs of a power supply is provided with an adjustment potentiometer on the front panel. In addition, the 15 VDC power supply units have an indicator light and test jacks on the front panel. (The voltages supplied by the triple voltage power supplies used for IEEE STD 796 circuit cards, have test jacks mounted on the associated M Card chassis.)

Loss of the DC power supply chassis can cause dependent board failure. Effects of this are a partial trip/actuation for IPC applications. For ESFAC and logic cabinet applications, single failures have no effect due to redundancy in the logic cabinet design. Detected faults are bypassed, and the remaining channels continue operation.

4.5.2 Cabinet cooling assembly (AUB)

The Cabinet Cooling Assembly is a modular assembly, mounted at the top front of an instrument cabinet to provide movement of cooling air throughout the cabinet. Each cabinet cooling assembly contains [ ]$^{(a,c)}$ centrifugal blowers or [ ]$^{(a,c)}$ cooling fans, each operating from a separate AC power source.

Power connections are made by means of modular connectors at the rear of the Cabinet Cooling Assembly. These connectors are assembled and keyed in such a fashion that only an identical unit, with the same input can be connected in place of a removed unit.

Failure of the cooling assembly can cause elevated temperatures in the respective cabinet. Note that the cabinets can still operate without active cooling (not for prolonged periods of time), but that the lifespan of the electronics is improved with cooling.

4.5.3 Power Distribution Assembly (APP)

The Power L:stribution Assembly filters, distributes, and sequences incoming AC power for an irdividual instrument cabinet. The assembly consists of a chassis, into which [ ]$^{(a,c)}$ Power distribution modules are fitted. Each module contains all the electrical components required for filtering, power-on sequencing, and branch circuit overcurrent protection for [ ]$^{(a,c)}$ separate branch circuits.

[

]$^{(a,c)}$

Failure of the power distribution assembly can cause dependent board failure. Effects of this are a partial trip/actuation for IPC applications. For ESFAC and logic cabinet applications, single failures have no effect due to redundancy in the logic cabinet design.

4.6 Nuisance Failures and Cascading Failures

The IPC has a single power feed. A partial trip could occur if power were lost to one division. Trip logic would be as follows:

- 2/3 logic in ESF
- 1/3 in reactor trip subsystem

2/4 reactor trip breakers would remain; the other sets would be in bypass. A concurrent failure could initiate a plant trip.

End devices could possibly be actuated by certain failures (nuisance failures).

The possibility of cascading failures arising from a single failure in the protection system was considered. Due to the isolation and the fail-safe design of the protection system, no possible cascading failures were identified. No failures were identified which could disable multiple channels.

5. Identification of failure categories

Possible failure modes include:

- Failed high
- Failed low
- Failed open
- Failed closed
- Random Access Memory (RAM) error
- Read Only Memory (ROM) error
- Programmable Array Logic (PAL) error
- Multiplexer error
- Bus interface error
- Central Processing Unit (CPU) error
- Timer error
- Power supply or interface fault
- Input/output error

All these may be summarized by "board fault". Consequences arising from each failure mode are discussed if they are unique.

6. Description of environmental conditions

All the I&C systems are located in ground benign conditions (per Mil Hdbk 217). Fires, floods, seismic events, etc. are analyzed separately in the PRA, and were found to be negligible contributors to risk, due to the design of the passive systems which respond in the event of an accident, and the spatial separation of these systems in the design. However, the passive plant design employs features to minimize risk, such as separation of protection channels, so that the effects from a single event are minimized. Effects from a site-wide event are analyzed in the seismic margins assessment, found in the AP600 Standard Safety Analysis Report.

7. Conclusions

A failure modes and effects analysis was performed on the protection system, and is shown in Table 2. The multiple protection channels, diversity, and fail-safe design of the protection system preclude single-point failures. Through the process of examining all feasible failure modes, it is concluded that the advanced passive plant protection system maintains all safety functions during single point failures.

8. References

1. AP600 Instrumentation and Control Hardware Description, WCAP-13382, R0, Westinghouse Electric Corporation, May 1992.

2. ANSI/IEEE Std. 352-1987, "General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems."

3. IEEE Std. 577-1976 "IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Power Generating Stations"

4. AP600 Instrumentation and Control Defense-in-Depth and Diversity Report, WCAP-13633, April 1993.

Table 1: Boards Used in Protection System

CARD DESCRIPTION	STYLE	IPC-RT	IPC-ESF	ESFAC	LOGIC CAB
[					]$^{(a,c)}$
[					]$^{(a,c)}$
[					]$^{(a,c)}$
[					]$^{(a,c)}$
[					]$^{(a,c)}$
[					]$^{(a,c)}$
					]$^{(a,c)}$
[					]$^{(a,c)}$
[					]$^{(a,c)}$
[					]$^{(a,c)}$
[					]$^{(a,c)}$
[					]$^{(a,c)}$
[					]$^{(a,c)}$
[					]$^{(a,c)}$
[					]$^{(a,c)}$
[					]$^{(a,c)}$
[					]$^{(a,c)}$
[					]$^{(a,c)}$
[					]$^{(a,c)}$
[					]$^{(a,c)}$
[					]$^{(a,c)}$
[					]$^{(a,c)}$

CARD DESCRIPTION	STYLE	IPC-RT	IPC-ESF	ESFAC	LOGIC CAB
[					]$^{(a,c)}$
[					]$^{(a,c)}$
[					]$^{(a,c)}$
[					]$^{(a,c)}$
[					]$^{(a,c)}$
[					]$^{(a,c)}$
[					]$^{(a,c)}$
[					]$^{(a,c)}$
[					]$^{(a,c)}$
[					]$^{(a,c)}$
[					]$^{(a,c)}$
[					]$^{(a,c)}$
Notes					
1. For Manual System Level Actuation					

Table 2: FMEA of Advanced Passive Plant Protection System

NAME	FAILURE MODE	METHOD OF DETECTION	EFFECT ON PROTECTION SYSTEM
1. Functional Processor (M12)			
1a	Functional failures - failures which corrupt normal sequential processing of main loop code	[ ]$^{(c)}$	Failed channel bypassed, inadvertent partial trip or partial actuation, partial trip failure or partial actuation failure for IPC applications. These will have no effect on plant operation due to the 2/4 logic and the presence of three remaining channels. For ESFAC applications, failures would have no effect due to fault tolerance in logic cabinet design, accomplished by means of failure detection and corrective actions. Redundant design allows the three remaining channels to continue operation.

FMEA of Advanced Passive Plant Protection System

Westinghouse Proprietary Class 3

NAME	FAILURE MODE	METHOD OF DETECTION	EFFECT ON PROTECTION SYSTEM
1b	Data failures - failures which do not inhibit the main loop processing, but alter the input and output data which is needed and produced by the main loop code	[ ]$^{(c)}$	Failed channel bypassed, inadvertent partial trip or partial actuation, partial trip failure or partial actuation failure for IPC applications. These failures will have no effect on plant operation due to the 2/4 logic and the presence of three remaining channels. For ESFAC applications, detectable failure would have no effect due to fault tolerance in logic cabinet design, accomplished by means of failure detection and corrective actions. Redundant design allows the three remaining channels to continue operation.

NAME	FAILURE MODE	METHOD OF DETECTION	EFFECT ON PROTECTION SYSTEM
1c	CMOS and PAL logic failures	[ ]$^{(c)}$	Failed channel bypassed, inadvertent partial trip or partial actuation, partial trip failure or partial actuation failure for IPC applications. These failures will have no effect on plant operation due to the 2/4 logic and the presence of three remaining channels. For ESFAC applications, detectable failure would have no effect due to fault tolerance in logic cabinet design, accomplished by means of failure detection and corrective actions. Redundant design allows the three remaining channels to continue operation.
2. Logic Processor (M03)	Same as for functional processor.	[ ]$^{(c)}$	Single M03 failures would have no effect on plant operation, due to fault tolerance in logic cabinet design, accomplished by means of failure detection and corrective actions. Redundant design allows the three remaining channels to continue operation.

NAME	FAILURE MODE	METHOD OF DETECTION	EFFECT ON PROTECTION SYSTEM
3. Data Highway Controller (M51)	Failure of message transfer, message altered in shared memory, failure of message transfer from shared memory to output port, message corrupted, or message altered in shared memory.	[ ]$^{(c)}$	Single failures have no effect due to fault tolerance in logic cabinet design, accomplished by means of failure detection and corrective actions. Redundant design allows the three remaining channels to continue operation.
4. Parallel I/O board (M19)	Bus failure, board failure	[ ]$^{(c)}$	Failure of this board can result in bus failure, and can result in a partial trip or partial actuation, depending on the microprocessor subsystem in which the board is used.
5. Isolated Parallel I/O board (M56)	Board failure	[ ]$^{(c)}$	Failure of this board can cause a bus failure, and can result in a partial trip or partial actuation, depending on the microprocessor subsystem in which the board is used.
6. Analog Input Processor (M40)	Board failure	[ ]$^{(c)}$	Failure of this board can cause a partial trip or partial actuation, depending on the microprocessor subsystem in which the board is used.

NAME	FAILURE MODE	METHOD OF DETECTION	EFFECT ON PROTECTION SYSTEM
7. Universal Memory Expansion board (M28)	Board failure	[ ]$^{(c)}$	Failed channel bypassed, inadvertent partial trip or partial actuation, partial trip failure or partial actuation failure for IPC applications. These will have no effect on plant operation due to the 2/4 logic and the presence of three remaining channels. For ESFAC applications, detectable failure would have no effect due to logic cabinet design, accomplished by means of failure detection and corrective actions. Redundant design allows the three remaining channels to continue operation.

FMEA of Advanced Passive Plant Protection System

Westinghouse Proprietary Class 3

NAME	FAILURE MODE	METHOD OF DETECTION	EFFECT ON PROTECTION SYSTEM
8. Serial Communications Controller (M48)	Board failure - data failure	[ ]$^{(c)}$	Possible effects of M48 failures for IPC usage are inadvertent trip or inadvertent partial actuation, partial trip failure, or partial actuation failure. For ESFAC applications, single failures have no effect due to fault tolerance in logic cabinet design, accomplished by means of failure detection and corrective actions. Redundant design allows the three remaining channels to continue operation.
9. Analog input board (EAI)	Board failure	[ ]$^{(c)}$	Failure of this board can cause a partial trip or partial actuation, depending on the subsystem in which the board is used. See Table 1 for board application details.
10. RTD Input Board (ERI)	Board failure	[ ]$^{(c)}$	Failure of this board can cause a partial trip or partial actuation, depending on the subsystem in which the board is used. See Table 1 for board application details.

NAME	FAILURE MODE	METHOD OF DETECTION	EFFECT ON PROTECTION SYSTEM
11. Digital (contact) Input board (ECI)	Board failure	[ ]$^{(c)}$	Failure of this board can cause a partial trip or partial actuation, depending on the subsystem in which the board is used. See Table 1 for board application details.
12. Digital (contact) output board (ECO)	Board failure, transmission failure	[ ]$^{(c)}$	Failure of this board can cause a partial trip.
13. Reactor Coolant Pump (RCP) Speed Sensor Input Board (ESI)	Board failure	[ ]$^{(c)}$	Failure of this board can cause a partial trip.
14. Power Interface (2/3 voted) Output board (EPO)	Board failure	[ ]$^{(c)}$	Failure of this board can cause inadvertent actuation of actuation failure of end device.
15. Power Interface Relay Driver board (EPR)	Board failure	[ ]$^{(c)}$	Failure of this board can cause inadvertent actuation of actuation failure of end device.

NAME	FAILURE MODE	METHOD OF DETECTION	EFFECT ON PROTECTION SYSTEM
16. Power Interface (Contact) Input Board (EPI)	Board failure	[ ]$^{(c)}$	Failure of this board can cause inadvertent actuation or actuation failure of end device.
17. Optical Datalink Transmitter board (ETX)	Board failure, transmission failure	[ ]$^{(c)}$	Failure of this board can cause a partial trip or partial actuation, depending on the subsystem in which the board is used. See Table 1 for board application details.
18. Optical Datalink Receiver board (ERX)	Board failure, receiver failure	[ ]$^{(c)}$	Single failures of this board can cause a partial trip for IPC usage. For ESFAC usage, single failures of this board have no effect due to 2/4 logic in the ESFAC.
19. Data Highway Transceiver board (EHX)	Board failure	[ ]$^{(c)}$	Single failures of this board have no effect due to fault tolerance in logic cabinet design, accomplished by means of failure detection and corrective actions. Redundant design allows the three remaining channels to continue operation.

FMEA of Advanced Passive Plant Protection System

Westinghouse Proprietary Class 3

NAME	FAILURE MODE	METHOD OF DETECTION	EFFECT ON PROTECTION SYSTEM
20. I/O Bus Extender Board (EBE)	Board failure	[ ]$^{(e)}$	Failure of this board can cause inadvertent actuation or actuation failure of end devices.
21. I/O Bus Selector board (XTS)	Board failure	[ ]$^{(e)}$	Single failures of this board have no effect due to fault tolerance in logic cabinet design, accomplished by means of failure detection and corrective actions. Redundant design allows the three remaining channels to continue operation.
22. Dynamic Trip Bus Clock Unit (DCU)	Board failure	[ ]$^{(e)}$	Failure of this board can cause a partial trip.
23. Dynamic Trip Bus Logic Unit (DLU)	Board failure	[ ]$^{(e)}$	Failure of this board can cause a partial trip.
24. Power Converter Board (EPC)	Board failure	[ ]$^{(e)}$	Failure of this board can cause a partial trip.

NAME	FAILURE MODE	METHOD OF DETECTION	EFFECT ON PROTECTION SYSTEM
25. Source Range Instrumentation	Instrumentation or board failure	[ ]$^{(c)}$	A partial trip could be initiated.
26. Intermediate Range Instrumentation	Instrumentation or board failure	[ ]$^{(c)}$	A partial trip could be initiated.
27. Power Range Instrumentation	Instrumentation or board failure	[ ]$^{(c)}$	A partial trip could be initiated.
28. High Voltage Power Supply (DNH)	Board failure	[ ]$^{(c)}$	Signal failure or a wrong output could be generated, resulting in a partial trip.
29. Low Voltage Power Supply (DNL)	Board failure	[ ]$^{(c)}$	Signal failure or a wrong output could be generated, resulting in a partial trip.
30. Nuclear Instrumentation Amplifier Modules (DNI)	Board failure	[ ]$^{(c)}$	A signal failure or wrong output could be generated, resulting in a partial trip.
31. Source Range Preamplifier (AAS)	Pre-amp failure (board failure)	[ ]$^{(c)}$	Failure of the source range preamplifier could cause a partial trip.

NAME	FAILURE MODE	METHOD OF DETECTION	EFFECT ON PROTECTION SYSTEM
32. DC Power Supply Chassis (ACP)	Power supply failure	[ ]$^{(c)}$	Failure can cause dependent board failure. An inadvertent partial trip or inadvertent partial actuation failure can result for IPC applications. For ESFAC and logic cabinet applications, single failures have no effect due to redundancy in the logic cabinet design. Failures are detected, and corrective actions taken. Redundant design allows the three remaining channels to continue operation.
33. Cabinet Cooling Assembly (AUB)	Power supply failure, filter plugs.	[ ]$^{(c)}$	Dependent cabinet could operate for a period of time with elevated temperature (not prolonged).

NAME	FAILURE MODE	METHOD OF DETECTION	EFFECT ON PROTECTION SYSTEM
34. Power Distribution Assembly (APP)	Power supply failure	[ ]$^{(c)}$	Failure can cause dependent board failure. Possible effects of these failures for IPC usage are inadvertent partial trip or inadvertent partial actuation. For ESFAC and logic cabinet applications, single failures due to fault tolerance in logic cabinet design, accomplished by means of failure detection and corrective actions. Redundant design allows the three remaining channels to continue operation.
35. Sensors	Fail high, fail low, fail as-is, drift high or drift low.	[ ]$^{(c)}$	A single sensor can be used for multiple functions, such as reactor trip, ESF, DAS, QDPS, or validation. Failed channel would be alarmed and bypassed.

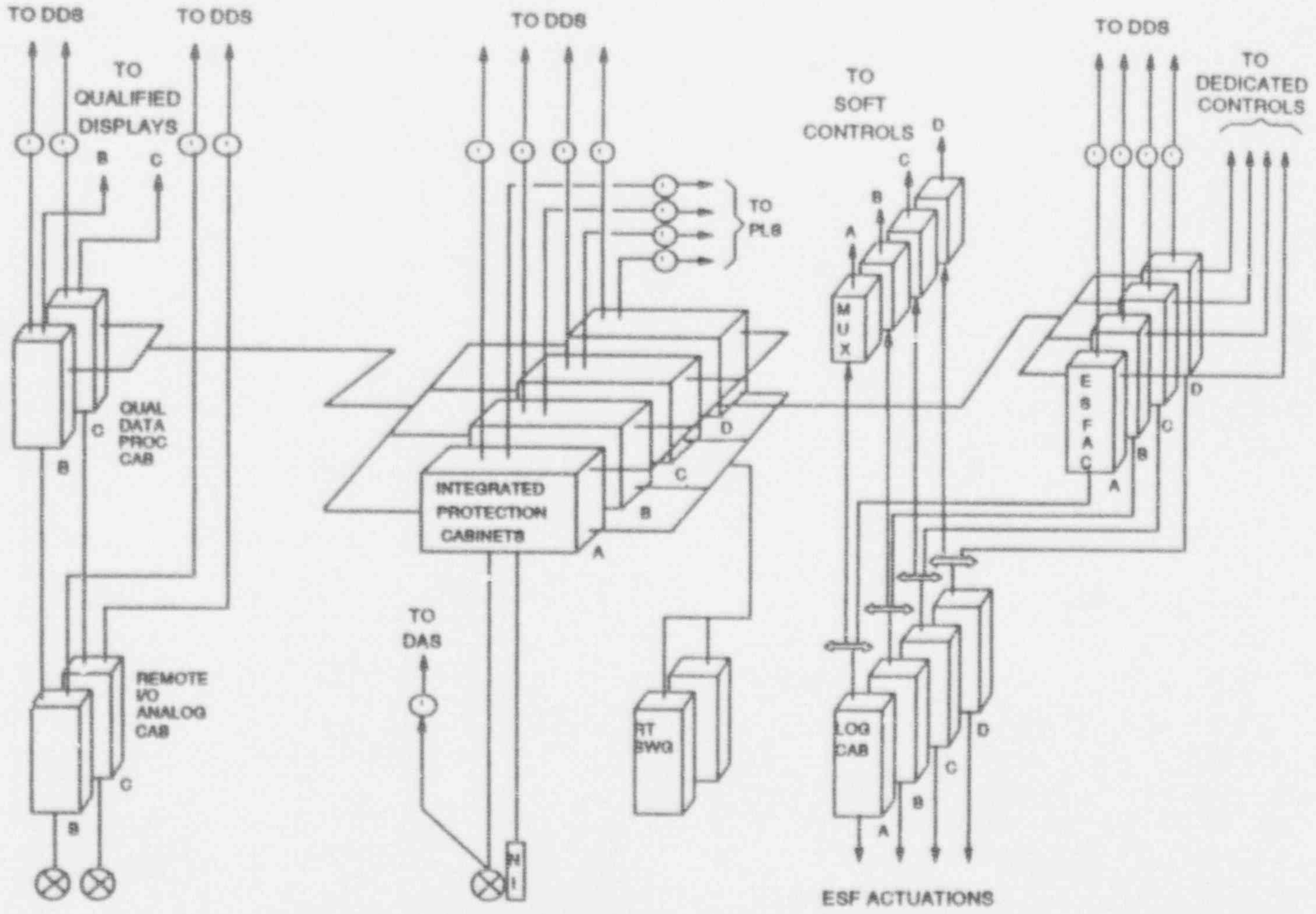

FIGURE 1: PROTECTION AND SAFETY MONITORING SYSTEM (PMS) ARCHITECTURE

THIS FIGURE IS FOR ILLUSTRATIVE PURPOSES ONLY

a,c

Figure 2 : Protection and Safety Monitoring System

a,c

Figure 3: Engineered Safety Features (ESF) Subsystem

FILE ESF DRW SK - 02/10/93

a,c

Figure 4: Reactor Trip Subsystem.

FILE RT.DRW SK 02/10/93

a,c

Figure 5: Global Trip Subsystem.

FILE GT.DRW SK · 04/07/93

a,c

Figure 6: Trip Enable Subsystem.

FILE TE DRW SK 02/10/93

a,c

Figure 7: Nuclear Instrumentation Signals Processing and Control (NISPAC)

FILE NISPAC DRW SK 02/10/93

a,c

Figure 8: Dynamic Trip Bus - Intermediate Level Functional Block Diagram

FILE DTB IL.DRW SK - 04/07/93