

ATTACHMENT 1

Letter from Mark L. Marchi (WPSC)

To

Document Control Desk (NRC)

Dated

November 23, 1999

Reactor Protection and Engineered Safety Features Upgrade
“Outline of the Reliability Report for Kewaunee Protection System Upgrade”

Non-Proprietary Class 3

**OUTLINE OF THE RELIABILITY REPORT FOR
KEWAUNEE PROTECTION SYSTEM
UPGRADE BY WESTINGHOUSE**

WPS-FMEA-001

Revision 1

November, 1999

Prepared by

**Selim Sancaktar
John Kitzmiller**

**Reliability and Risk Assessment Group
Nuclear Services Division
Westinghouse Electric Company LLC**

This document is the property of and contains proprietary information owned by Westinghouse Electric Company and/or its subcontractors and suppliers. It is transmitted to you in confidence and trust, and you agree to treat this document in strict accordance with the terms and conditions of the agreement under which it was provided to you.

**Copyright © 1999
Westinghouse Electric Company LLC**

Table Of Contents

1.0 INTRODUCTION AND BACKGROUND4
1.1 Currently Operating RPS.....4
2.0 SYSTEM DESCRIPTION AND BOUNDARIES 9
3.0 MODEL ASSUMPTIONS AND OUTLINE.....21
4.0 FAILURE MODES AND EFFECTS ANALYSIS22
4.1 Introduction.....22
5.0 DATA BANK CONSTRUCTION29
5.1 Data Used29
6.0 REACTOR TRIP FAILURE PROBABILITY31
6.1 RPS Modeling Standard from NUREG/CR-550031
6.2 FTA Assumptions31
6.3 Fault Tree Top Logic.....32
6.4 Fault Tree Model33
7.0 ENGINEERED SAFEGUARDS ACTUATION FAILURE PROBABILITY34
7.1 FTA Assumptions34
7.2 FTA Top Logic34
7.3 Fault Tree Model34
8.0 SENSITIVITY ANALYSES35
8.1 Reactor Trip Without Diverse Actuation Signals.....35
8.2 Effect Of AMSAC On System Reliability.....35
9.0 SUMMARY, CONCLUSIONS, AND INSIGHTS.....36
10.0 REFERENCES37

List of Tables

Figure 1-1 Existing Kewaunee RPS System 7
Figure 1-2 Existing Kewaunee ESFAS System 8
Table 1 Representative Westinghouse RPS trip Signals from NUREG/CR-5500 12
Figures 2 and 3. Westinghouse RPS simplified diagram from NUREG/CR-5500 18
4-1 List I&C Components and Their Failure Modes 26
Figure 4-2 Failure Modes and Effects Analysis (an illustration) 28
Table 5-1 Data Bank 30

ACRONYMS

| | |
|-------|---|
| CDF | (Plant) Core Damage Frequency |
| DBE | Design Basis Earthquake |
| IPEEE | Individual Plant Evaluation for External Events |
| LERF | Large Early (Fission Product) Release Frequency |
| OBE | Operating Basis Earthquake |
| PRA | Probabilistic Risk Assessment |
| PSA | Probabilistic Safety Assessment (interchangeably used with PRA) |
| RCS | Reactor Coolant System |
| RHR | Residual Heat Removal (pumps; system) |
| CCF | Common Cause Failure |
| DAS | ATWS Mitigation and Diverse Actuation Circuitry |
| FMEA | Failure Modes and Effects Analysis |
| FT | Fault Tree |
| FTA | Fault Tree Analysis |
| CRDM | Control Rod Drive Mechanism |
| SI | Safety Injection |
| RPS | Reactor Protection System |
| RTS | Reactor Trip System |
| ESFAS | Engineered Safety Features Actuation System |
| DNBR | Departure from Nucleate Boiling Ration |
| BO | Blackout |
| AFW | Auxiliary Feedwater |
| DG | Diesel Generator |
| SW | Service Water |
| ICS | Internal Containment Spray |
| I&C | Instrumentation and Control |

OUTLINE OF THE RELIABILITY REPORT FOR KEWAUNEE PROTECTION SYSTEM UPGRADE BY WESTINGHOUSE

1.0 INTRODUCTION AND BACKGROUND

A limited scope upgrade of the Kewaunee Nuclear Power Plant protection system is being considered. This includes the reactor protection system (RPS) and the engineered safety systems actuation system (ESFAS). This report defines the scope of a reliability study of the upgraded RPS; the actual analysis will be done when the system drawings are available.

The currently operating system function is summarized below. The upgrade is discussed in the next section.

1.1 Currently Operating RPS

The information in this section comes primarily from the Kewaunee Nuclear Power Plant Updated Safety Analysis Report (Reference 5). Additional references are cited where applicable.

The RPS and ESFAS are designed to meet the single failure criterion of the General Design Criteria for nuclear power plants and is optimized to provide reactor trip and safeguards actuation functions for various postulated plant accidents. Fail-safe design features ensure that necessary protective actions are still initiated following a single failure within the RPS, but these features can produce spurious SI initiating events upon failure of specific individual components (e.g., multiple process instrument channel failures that satisfy SI actuation logic).

The overall protection system consists of: Foxboro process protection instrumentation system, nuclear instrumentation system, reactor protection and safeguards logic relay cabinets, SI sequencer, and reactor trip switchgear. For reactor trip and engineered safety features actuation, the safeguards and reactor protection logic relay cabinets each contain two redundant logic trains, A and B, that are physically and electrically independent. The logic relay cabinets receive inputs from process instrumentation, nuclear instrumentation, field contacts, and directly from main control board switches.

Both physical and electrical separation of redundant analog channels is maintained from the process sensors through the instrumentation channels in the Foxboro process racks using separate cable trays, conduit, and penetrations. This separation continues into the safeguards and reactor protection relay racks for both logic trains using separate cable trays to carry the interconnecting wiring between the bistable outputs and the logic relay racks. This also permits total electrical and physical separation between logic train A and train B. Train independence is maintained from the logic trains out to their respective engineered safety features components and reactor trip breakers. Simplified diagrams of RPS and ESFAS are shown in Figures 1-1 and 1.2.

The protective actions initiated by the protection systems are broadly classified into two major categories, reactor trips and actuations of engineered safety features. Therefore, the protective functions are addressed from two functionally defined subsystems, the reactor protection system (RPS) and the engineered safety features actuation system (ESFAS). These two subsystems perform all of the safety-related actions associated with the protection system.

The RPS functions to prevent reactor operation outside of prescribed safe operating limits. The limits of safe reactor operation are defined by the correlation of reactor power, Reactor Coolant System temperatures, pressure, and flow, pressurizer level and secondary system heat removal capability. The reactor operating philosophy is to define an allowable region of power, pressure and coolant temperature conditions. This allowable region is defined by the three primary tripping functions: the overpower delta-T trip, the over-temperature delta-T trip and the nuclear overpower trip. The operating region below these trip settings is designed so that no combination of power, temperature, and pressure could result in departure from nucleate boiling ratio (DNBR) less than 1.3 for any credible operational transient with all reactor coolant pumps in operation. Additional tripping functions to those stated above are provided to back up the primary tripping functions for specific abnormal conditions.

Rapid reactivity shutdown is provided by the insertion of rod cluster control assemblies (RCCA) by free fall. Duplicate series-connected circuit breakers supply all power to the control rod drive mechanisms (CRDM). The CRDM must be energized for the RCCA to remain withdrawn from the core. Automatic reactor trip occurs upon loss of power to the CRDM. If the RPS receives signals indicative of an approach to unsafe operating conditions, the system actuates alarms, prevents control rod withdrawal, initiates load runback, and/or opens the reactor trip breakers. At various power levels, permissive signals are generated which permit the operator to block certain reactor trip signals when they are not required for safety.

In addition to the requirements for a reactor trip for anticipated abnormal transients, the plant is

Westinghouse Non-Proprietary Class 3

provided with adequate instrumentation and controls to sense accident situations and initiate the operation of necessary engineered safety features. The occurrence of a limiting fault, such as a loss of coolant accident or a steam line break, requires a reactor trip plus actuation of one or more of the engineered safety features (ESFs) in order to prevent or mitigate damage to the core and reactor coolant system components, and ensure containment integrity.

Generation of a safety injection (SI) actuation signal results in a reactor trip, feedwater and containment isolation and emergency diesel generator startup. Once an SI signal is generated, the SI sequencer sequentially energizes safeguards equipment providing that power is available for the associated ESF bus and no conflict exists between blackout (BO) and SI sequences. This is to ensure proper loading of the diesel generators in the event that outside power supplies to the safeguards buses (5 and 6) are interrupted and the diesel generators assume the loads on these buses. Equipment energized by the SI sequencer includes: SI pumps, residual heat removal (RHR) pumps, internal containment spray (ICS) pumps (if diesel generator (DG) is supplying and a hi-hi containment pressure signal exists), shield building ventilation, service water (SW) pumps, containment fan coil units and dome fan, auxiliary feedwater (AFW) pumps, component cooling pumps, instrument air compressors, control room post-accident recirculation and auxiliary building special ventilation, and safeguard fan coil units.

Westinghouse Non-Proprietary Class 3

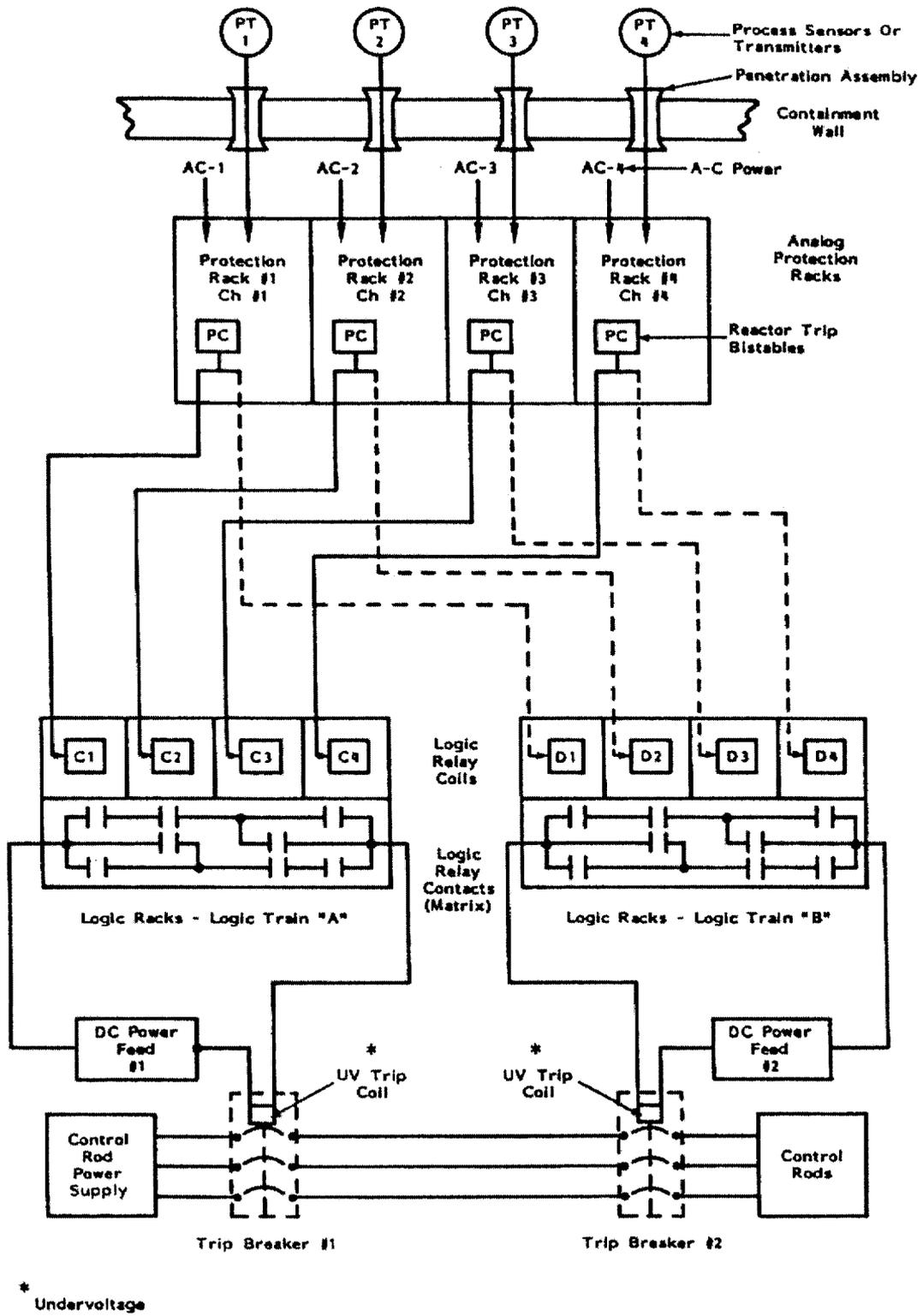


Figure 1-1 Existing Kewaunee RPS System

Westinghouse Non-Proprietary Class 3

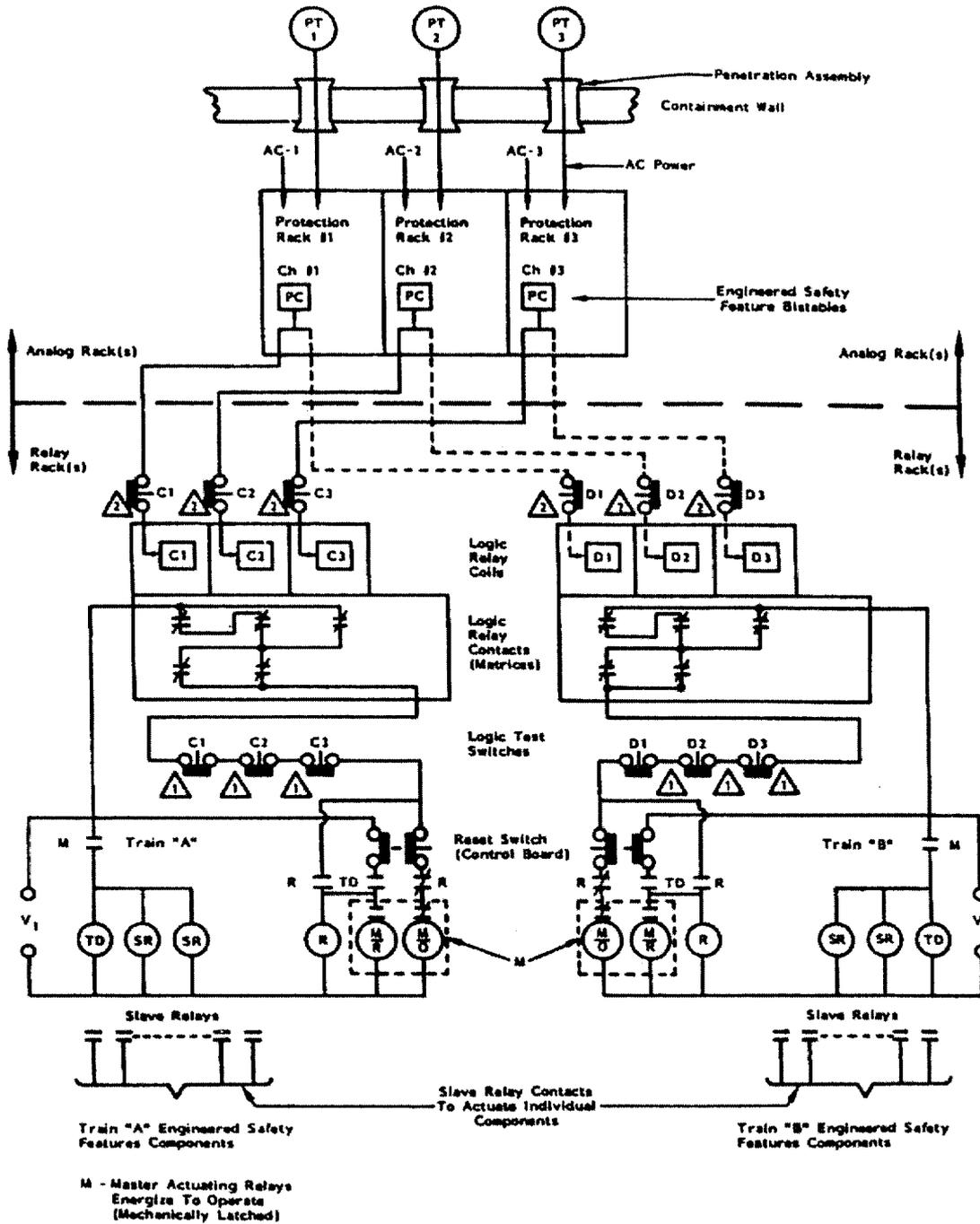


Figure 1-2 Existing Kewaunee ESFAS System

2.0 SYSTEM DESCRIPTION AND BOUNDARIES

Out of the existing plant protection and control systems, only the RPS and ESFAS are affected by the upgrade. The upgraded system can be outlined as follows:

1. Reactor Protection and ESF Actuation System;
2. ATWS Mitigation and Diverse Actuation Circuitry (DAS);
3. Ovation system for information transmittal.

The sensors, and the reactor trip breaker circuitry are outside the upgrade scope.

More information about the system upgrade architecture can be found in Reference 6.

Figure 2-1 outlines the system in this preliminary stage. More information about the system upgrade architecture can be found in Reference 6.

The power (AC) support to the cabinets is also outside the scope of the upgrade.

The manual interfaces are not in the scope of the upgrade.

The following plant I&C related systems are not in the scope of the upgrade:

1. Nuclear Instrumentation System (NIS)
2. Automatic and Manual Control Systems:
 - Pressurizer level Control
 - Pressurizer Pressure Control
 - Reactor Rod Control
 - S/G Level Control
 - Turbine/Generator Control
 - Steam Dump Control
3. RCP Bus Undervoltage and Underfrequency System.

2.1 System Description

2.1.1 System Operation

The Westinghouse RPS is a complex control system comprising numerous electronic components that combine to provide the ability to produce an automatic or manual rapid shutdown of the nuclear reactor, known as a reactor trip or scram. In spite of its complexity, the Westinghouse RPS can be roughly divided into four segments--rods, trip breakers, logic cabinet (containing the two trains of the RPS), and instrumentation rack--as shown in Figure 1. The rods segment includes the rod control cluster assemblies (RCCAs) and control rod drive mechanisms (CRDMs). Westinghouse RPSs typically have 40 to 60 RCCAs and associated CRDMs. The trip breaker segment includes the reactor trip breakers and .. associated undervoltage devices and shunt trip devices. Most of the Westinghouse RPSs have DB-50 type reactor trip breakers, while some of the newer plants have DS-416 versions. For the logic cabinet, approximately 70% of the RPSs have solid state logic termed the Solid State Protection System (SSPS), while the remaining 30% have analog logic. Finally, for the instrumentation rack approximately 85% of the RPSs have analog systems to process the signals, while the remaining 15% have converted to the Eagle-21 solid state system.

| RPS Segments | | | |
|--|--------------------------------|---|-------------------------------------|
| Instrumentation Rack | Logic Cabinet | Trip Breakers | Rods |
| Generally, 3 channels for 3-loop plants, 4 channels for 2- and 4-loop plants; analog (Analog Series 7300 or earlier) or Eagle-21 signal processing (note that the sensors are located within containment rather than in the instrumentation racks) | 2 trains; SSPS or analog logic | 2 reactor trip breakers (and 2 bypass breakers); DB-50 or DS-416 design; automated shunt trip and undervoltage trip | 40 to 60 RCCAs and associated CRDMs |

Figure 1. Segments of Westinghouse RPS.

The analysis of the Westinghouse RPS is based on a four-loop plant with either an Eagle-21 or Analog Series 7300 sensor processing system and an SSPS for the logic cabinet. This configuration has been used in genetic analyses of Westinghouse RPSs as representative of most designs.^{10 11} A simplified diagram of the SSPS/Analog Series 7300 design is presented in Figure 2. The SSPS/Eagle-21 modification is shown in Figure 3. The following discussions

concerning system operation and system testing refer to the SSPS/Analog Series 7300 RPS design. The SSPS/Eagle-21 design is covered in Section 2.1.3.

In Figure 2, there are two RPS trains in the logic cabinet, trains A and B. These trains receive trip signals from the channels, process the signals, and then open the reactor trip breakers (RTBs) given appropriate combinations of signals from the channels. The channel portion of the RPS includes many different types of trip signals, as indicated in Table 1.¹² The trip signals include various neutron flux indications, pressurizer pressure and level, reactor coolant flow, steam generator level, and others. Several of the signals involve measurements in each of the four loops of the reactor, with a trip signal being generated if at least two of the four loop measurements exceed a setpoint. Shown in the simplified RPS diagram in Figure 2 are sensor/transmitters and signal processing modules associated with the overpower AT and pressurizer high pressure trip signals. (These two signals, along with others, protect the plant from uncontrolled rod withdrawal transients while at power.¹²) For each loop there are cold leg and hot leg coolant temperature sensor/transmitters that combine to determine the loop ΔT and T_{average} . This information, along with flux information (not shown in Figure 2), is converted by the processing module and sent to the associated bistable, which trips if the bistable setpoint is reached. Similarly, there are four pressure sensor/transmitters for the pressurizer, one for each channel. The pressure processing module converts the pressure signal and sends it to the associated bistable.

The logic cabinet or SSPS in Figure 2 includes two trains. When a bistable in the instrumentation rack trips, it actuates associated relays in both of the trains. The solid state logic module, or universal card, for that trip parameter (one in each train) then determines whether sufficient relays have actuated (i.e., two of four for pressurizer high pressure). If so, a trip signal is sent to the undervoltage driver card (one in each train), which then opens the RTB associated with that train.

In Figure 2, there are two normally-closed RTBs and two normally-open bypass trip breakers. The bypass trip breakers are used only when testing the reactor trip breakers. Train A of the RPS logic actuates RTB-A and train B of the logic actuates RTB-B. Opening of either RTB disconnects AC power from the rod control motor generator sets to the rod drive power cabinets, which results in the RCCAs dropping into the reactor core and shutting down the nuclear reaction. During plant operation, the normally-energized undervoltage coil maintains the RTB in a closed position. The shunt trip coil is normally de-energized. An undervoltage driver card trip signal results in de-energization of the undervoltage coil and energizing (through the auto shunt trip relay) of the shunt trip coil, either of which will open the RTB.

Table 1. Representative Westinghouse RPS trip Signals from NUREG/CR-5500.
A four-loop reactor design is assumed.

| Trip Signal | Trip Logic^a | Purpose of Trip |
|--|---|---|
| 1. Source range high neutron flux | 1 of 2 sensors | Prevent an inadvertent power increase while subcritical or at low power |
| 2. Intermediate range high neutron flux | 1 of 2 sensors | Prevent an inadvertent power increase at low power |
| 3. Power range high neutron flux (low setpoint) | 2 of 4 sensors | Prevent an inadvertent power increase while at power |
| 4. Power range high neutron flux (high setpoint) | 2 of 4 sensors | Limit maximum power level |
| 5. High positive rate, neutron flux | 2 of 4 sensors | Limit power excursions |
| 6. High negative rate, neutron flux | 2 of 4 sensors | Prevent unacceptable power distributions |
| 7. Overtemperature ΔT | 2 of 4 overtemperature ΔT signals (one for each loop) | Prevent operation with a $DNBR < 1.30^c$ |
| 8. Overpower ΔT^b | 2 of 4 overpower ΔT signals (one for each loop) | Prevent excessive power density |
| 9. Pressurizer low pressure | 2 of 4 sensors | Prevent $DNBR < 1.30^c$ |
| 10. Pressurizer high pressure ^b | 2 of 4 sensors | Protect integrity of reactor coolant system pressure boundary |
| 11. Pressurizer high water level | 2 of 3 sensors | Prevent solid water operations |
| 12. Low reactor coolant flow | 2 of 3 sensors in any one of the loops | Ensure adequate loop flow to remove core heat |
| 13. Reactor coolant pump undervoltage | 2 of 4 buses | Ensure adequate loop flow to remove core heat |
| 14. Reactor coolant pump underfrequency | 2 of 4 buses | Ensure adequate loop flow to remove core heat |

Westinghouse Non-Proprietary Class 3

| Trip Signal | Trip Logic ^a | Purpose of Trip |
|--|--|--|
| 15. Steam generator low water level (mismatch with steamflow/feedflow) | 1 of 2 level sensors coincident with 1 of 2 mismatches in the same steam generator | Anticipate loss of heat sink |
| 16. Turbine trip | 2 of 3 low autostop oil pressure or 4 of 4 turbine stop valves shut | Remove heat source if steam load is lost to steam generators |
| <p>a. A four-loop reactor design is assumed.</p> <p>b. These two signals are modeled in the RPS fault tree used for this study.</p> <p>c. DNBR = departure from nucleate boiling ratio</p> | | |

2.1.2 System Testing

RPS testing addresses the four segments of the RPS indicated in Figure 1. For RPS channels (instrumentation rack), there are typically four types of tests: channel checks (qualitative verification of instrument channel behavior) every 12 hours, quarterly (every three months) functional tests, calibration tests every refueling or 18 months, and time response tests every refueling or 18 months^{11,12}. Channel checks detect gross sensor/transmitter failures and drift. The functional tests for analog channels are performed using a test switch that aligns the channel input to test jacks (bypassing the sensor) and the output bistable to the test lamp. The test input signal is then increased until the bistable trips, as indicated by the test lamp. This test is repeated for each of the trip parameters feeding into the channel. Before 1986, this channel functional test was required to be performed monthly and involved putting the channel into a tripped condition (half reactor trip condition) during the test. However, in 1986 Westinghouse obtained approval to perform such tests quarterly, rather than monthly, and to place the channel into a bypass condition, rather than a tripped condition. (Some Westinghouse plants cannot place a channel into a bypass condition without jumpers or removing leads. In such cases the channel must be placed into a tripped condition.) It is not known when each Westinghouse plant switched from monthly to quarterly testing of the channels. This report assumes quarterly testing for all of the plants over the entire period 1984 through 1995. However, a sensitivity study, covers the assumption of monthly testing. The refueling or 18-month calibration tests cover the sensor/transmitters. Finally, the refueling or 18-month time response tests are similar to the quarterly functional tests, but include measurement of the time for the channel to respond to changes in inputs.

For the logic cabinet segment (train) of the RPS, two types of tests apply: staggered monthly -functional tests (each train tested every two months) and refueling or 18-month time response tests. The staggered monthly test essentially isolates the SSPS from the channels and places the train into a bypass condition. (A tripped condition would result in a reactor trip.) A semi-automatic test panel is used to generate all possible combinations of channel inputs and test the SSPS response up to, but not including, the RTB undervoltage and shunt trip coils. Before 1986, this test was performed bimonthly. However, by 1992 the testing routine had changed to staggered monthly.¹⁴ Both testing routines result in the same number of tests per year.

Two types of tests also apply to the RTBs and bypass trip breakers, similar to the logic cabinet tests. The staggered monthly functional test involves separate testing of the undervoltage and shunt trip coil mechanisms for opening the RTB, performed by using manual pushbuttons located near the RTBs. Before the RTB is tested, the associated bypass trip breaker is tested and placed into service (closed). During the test of the RTB, the associated train is in a bypass condition. This leaves only the other train available to respond to plant upset conditions. However,

this train actuates both the RTB and the associated bypass trip breaker, either of which can interrupt power to the rod drive power cabinets. After the test, the bypass trip breaker is removed from service. Similar to the SSPS, this test was performed bimonthly before 1986, but has since changed to staggered monthly. The time response test every refueling or 18 months measures the time the RTB requires to open.

Finally, the rod segment of the RPS involves two types of tests: monthly limited movement tests of each RCCA/CRDM, and RCCA drop timing tests every refueling or 18 months.

2.1.3 Eagle-21 Description

The Eagle-21 upgrade to the RPS, as modeled in this report and shown in Figure 3, replaces the channel process logic modules with an integrated, solid-state Eagle-21 module.¹³ Otherwise, the same sensor/transmitters and bistables are used. The Eagle-21 upgrade allows for increased on-line monitoring and diagnostics, and more efficient quarterly testing. The increased on-line monitoring results in most failures being detected almost instantaneously, rather than during quarterly testing.

2.1.4 System Boundary

The RPS boundary for this study includes the four segments indicated in Figures 1, 2, and 3: channels (instrumentation rack), logic cabinet, trip breakers, and rods. Also included is the control room operator who pushes the manual reactor trip button. The ATWS mitigation system AMSAC is not included.

2.2 System Fault Tree

This section contains a brief description of the Westinghouse RPS fault tree developed for this study. The analysis of the Westinghouse RPS is based on a four-loop plant with either an Eagle-21 or an Analog Series 7300 sensor processing system and an SSPS logic cabinet. As mentioned in Section 2.1.1, this configuration has been used in generic analyses of Westinghouse RPSs as representative of most of the various designs and configurations. It should be noted that the RPS fault tree development represents a moderate level of detail, reflecting the purpose of this project to collect actual RPS performance data and assemble the data into overall RPS unavailability estimates. The level of detail of the fault tree reflects the level of detail available from the component failure information in NPRDS and the LERs.

The top event in the RPS fault tree is "Reactor Protection System (RPS) Fails." RPS failure at this top level is defined as an insufficient number of RCCAs dropping into the core to inhibit the nuclear reaction. Various plant upset conditions can result in differing requirements for the minimum number of RCCAs to drop into the core, and the positions of the RCCAs within the core can also be important. The Seabrook Probabilistic Safety Assessment conservatively used two or more RCCAs failing to insert as the RPS failure criterion.¹⁵ Also, WASH-1400 conservatively used three or more RCCAs failing to insert. However, NUREG-0460 indicates for a specific Westinghouse reactor study, 25 RCCAs failing to insert will still result in a shutdown of the nuclear reaction for most initiating events and 10 RCCAs failing to insert will shutdown the nuclear reaction for almost all initiating events.¹ Therefore, the RCCA failure criterion might range from 2 to 25 RCCAs failing to insert into the core upon demand. The lower limit is very conservative, while the upper limit may not be appropriate given severe plant upset conditions or asymmetric patterns of RCCA failures. For this study, 10 or more RCCAs failing to fully insert into the core was chosen as the RPS failure criterion.

It should be noted that the structure of the RPS fault tree is independent of the selection of the number of RCCAs having to fail to insert into the core. For the rest of the fault tree, failure to remove power from the CRDMs results in all of the RCCAs failing to insert. Failure to remove power from the CRDMs results if both RTBs fail to open, if both SSPS trains fail to actuate the RTBs, or if three of four channels fail to generate reactor trip signals.

The level of detail in the RPS fault tree includes RTBs and bypass trip breakers (broken down into mechanical/electrical, undervoltage coil, and shunt trip coil), undervoltage driver and universal cards in the SSPS, selected relays, temperature and pressure sensor/transmitters, Eagle-21 and analog process logic modules, and bistables. The Eagle-21 and Analog Series 7300 RPS designs are distinguished by minor changes in the channel portion of the fault tree, with a house event used to mm on the applicable basic events. Within the channels, two trip parameters are modeled: overpower ΔT and pressurizer high pressure (see Table 1). These are two parameters that would detect an uncontrolled rod withdrawal transient while the plant is at power. In general, at least three RPS parameters are available to initiate a trip signal for any type of plant upset condition requiring a reactor trip. Only two parameters are included in the fault tree to simplify the tree.

Common-cause failures (CCFs) across similar components were explicitly modeled in the RPS fault tree. Examples of such components include the mechanical/electrical, undervoltage coil, and shunt trip coil portions of the RTBs and bypass trip breakers, undervoltage driver cards, universal cards, analog or Eagle-21 processors, sensor/transmitters, relays, and bistables. In general, the common-cause modeling in the RPS fault tree is limited to the events that fail enough

Westinghouse Non-Proprietary Class 3

components to fail that portion of the RPS. For example, for channels, three or four of four must fail in order for the RPS to fail to generate a reactor trip signal. Therefore, common-cause modeling for the channels includes such events as three or four out of four pressure signal processing modules failing. Lower order CCF events, such as two out of four components failing, are not modeled in the fault tree. Such events would have to be combined with an independent failure for the three out of four failure criterion to be met.

Test and maintenance outages and associated RPS configurations are modeled for RTB/SSPS and channel outages. For channel outages, the fault tree channel was developed assuming that a channel out for testing or maintenance is placed into the bypass mode, rather than a tripped mode. As mentioned earlier, Westinghouse obtained NRC approval for placing channels in bypass during testing or maintenance in 1986, as long as jumpers or lifting of leads is not needed in order to place the channel into bypass. Test and maintenance outages for all four channels are combined, for simplicity, into a single" outage event for channel A in the RPS fault tree. For RTB or SSPS train testing or maintenance, that train is placed into a bypass mode, so only the other train is available to respond to plant upset conditions. Train outages are modeled individually for trains A and B.

Figure 2 and 3 from Reference 1 are given below.

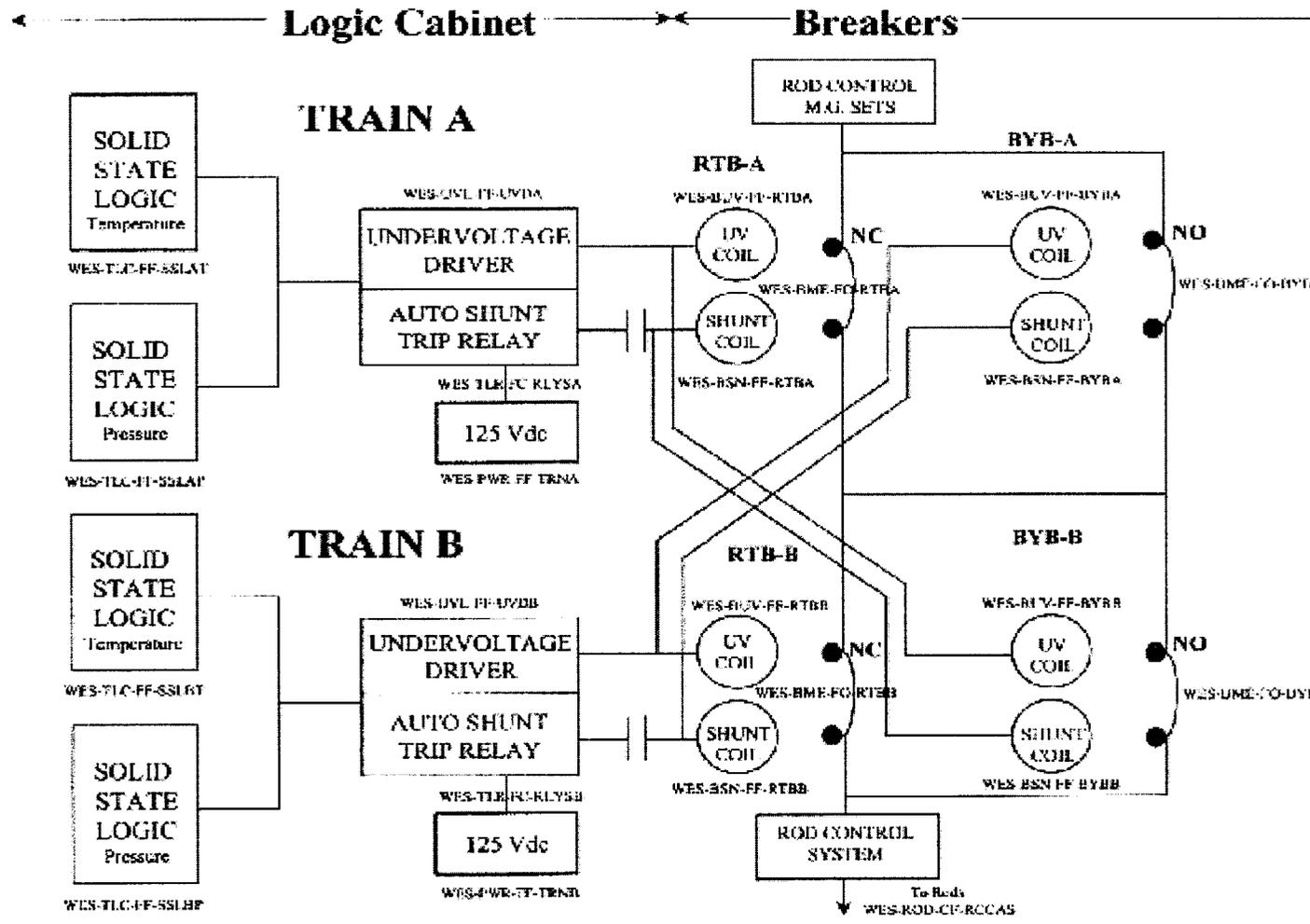


Figure 2. Westinghouse RPS simplified diagram (Analog Series 7300)

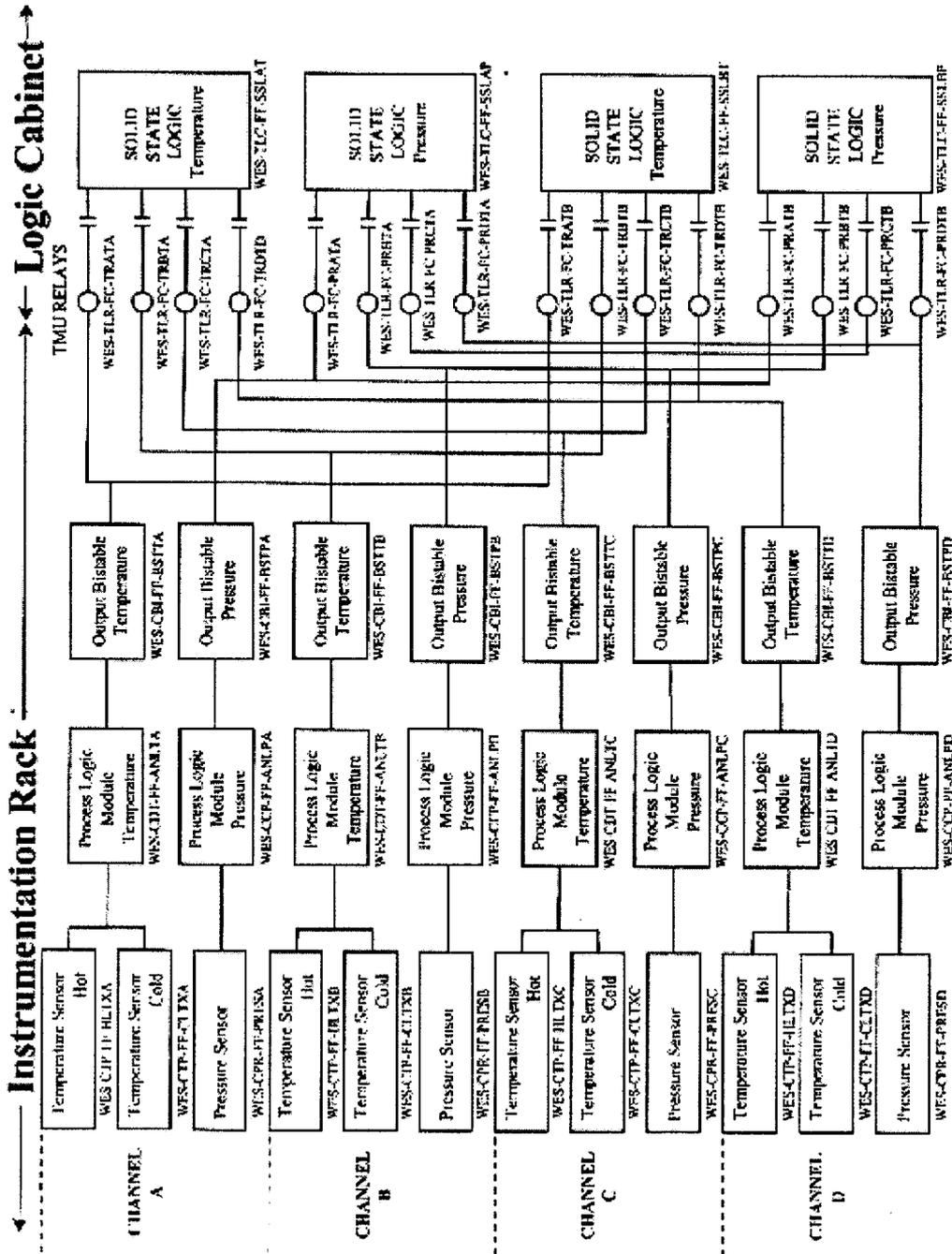


Figure 2. (continued).

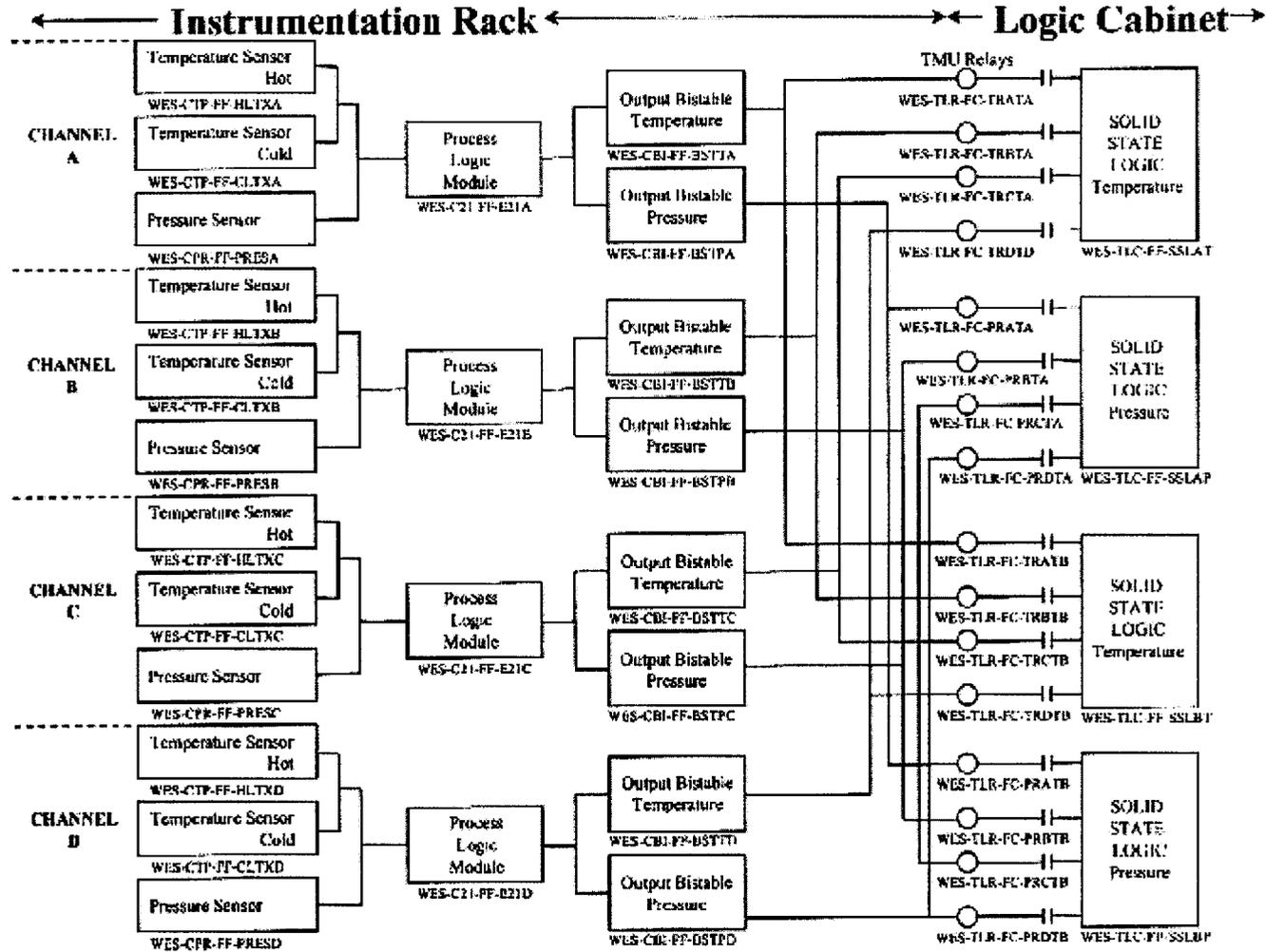


Figure 3. Westinghouse RPS simplified diagram (Eagle-21).

3.0 MODEL ASSUMPTIONS AND OUTLINE

In this report, a reliability analysis of the Kewaunee protection system is performed, both qualitatively and quantitatively, using failure modes and effects analysis (FMEA) and fault tree analysis (FTA).

The FMEA, which is a qualitative analysis, is presented in Section 4.

The I&C System failure probability is calculated using fault tree analysis methods. In order to make the models comparable to a standard model, the fault tree model created in NUREG/CR-5500, Volume 2 (Reference 1) is used as the reference, for system failure probability comparisons, basic event data input, and for construction of the fault tree logic. The fault tree model in Reference 1 is modified and supplemented as needed to generate an I&C failure model compatible with that of the Kewaunee upgrade.

Reference 1 offers only a failure model for one protection function, namely to trip the reactor. In the current report, two complementary functions (missions) of the I&C system are modeled in Sections 6 and 7. These functions are:

1. A reactor trip;
2. An engineered safeguards system actuation.

The results of a FTA may be sensitive to the definition of the system boundary. In this report, the system boundary is defined consistent with that of Reference 1, to allow comparison of the numerical results.

FTA results may also vary depending upon the data used. Since extensive data analysis has been performed and its results are provided in Reference 1, that data is used whenever possible; otherwise, actuarial data from similar operating I&C system is used when available; finally, generic data is used if no other data is available. The data bank so generated is given in Section 5.

4.0 FAILURE MODES AND EFFECTS ANALYSIS

4.1 Introduction

The Failure Mode and Effects Analysis (FMEA) (Reference 2) is a systematic procedure for identifying the *potential* failure modes of a component and to determine their consequences, i.e., effects on a system. The FMEA provides quick visibility of the most obvious failure modes and identifies potential single point failures.

The analysis approach used for the FMEA is dictated by variations in design complexity and the available data. Two primary approaches for accomplishing an FMEA are:

Functional Approach - recognizes that every item or combination of items is designed to perform specific functions that can be classified as outputs. The functional approach is typically utilized when the complexity of a system requires a top-down approach or when the hardware cannot be uniquely identified.

Hardware Approach - lists individual hardware items and analyzes their possible failure modes. The hardware approach is typically utilized when the hardware can be uniquely identified.

The "Hardware Approach" was selected for this reliability analysis of the reactor trip and ESF protection system. This approach lists the individual potential failure modes of major components that make up the system and aids in a systematic evaluation.

The boundary of this analysis (Kewaunee Process Protection System Upgrade) consists of only the hardware included within the Westinghouse I&C upgrade scope in which the E3 version of the Ovation system is to be used. Those systems and components that physically appear beyond the Westinghouse scope are excluded from this reliability investigation. A list of the components that constitute the I&C system is provided in Table 4-1.

For the purposes of this analysis the following definitions are used:

Failure - the termination of the ability of an item or equipment to perform its required function.

Westinghouse Non-Proprietary Class 3

Failure Cause - the physical, chemical or other process which results in failure or the circumstance that induces or begins the process which results in failure.

Failure Mode - the effect by which a failure is observed to occur.

The FMEA worksheet captures the failures and relevant information for each of the major system components and groups this information in categories of: component/assembly, function(s), potential failure mode(s) and cause(s), potential failure effect(s), and mitigating feature(s). These categories are described in the following paragraphs.

A list of potential components and their failure modes and causes to be included in the FMEA is contained in Table 4-1.

A. Component / Assembly

The component / assembly category contains the name of the component as well as a reference to drawing(s) for the component.

B. Function

The function category contains a brief description of the function(s) of the associated components.

C. Failure Mode and Cause

When failures occur in a system or component, they often occur in a variety of ways. For example, a relay can fail in a closed position or an open position. A failure mode is defined as: the effect by which a failure is observed to occur and is usually characterized by description of the manner in which a failure occurs. It is a description of the failure itself. A failure mode provides a descriptive characterization of the failure event in generic terms - not in terms of the failure cause which occurred and not in terms of the failure effect. Some failure modes used in this FMEA are:

**REACTOR TRIP AND ESF PROTECTION
SYSTEM COMPONENTS FAILURE**

| MODES |
|-------|
| Later |

Failure Cause

The failure cause defines the physics of the failure. This involves the description and sequence of those mechanical, electrical and chemical processes or a combination of these, which occurred during the period in which the failed item changed from an operational state to a failed state. The failure cause is the process or the beginning of the process or evolution of the phenomena that occurs to change the physical and/or functional characteristic of the materials in the failed item.

D. Failure Effects (Local and Plant)

The effects of a failure within a system may be propagated to higher and lower levels of assembly. Failure mode and effect analysis is a formal approach to the analysis of failure modes and their propagated effects and involves the loss or degradation of functions and also the effects of failures on system safety. It should be noted that as failure modes and effects occur at successively higher levels of indenture each failure effect may give rise to a new failure mode. For this analysis, the failure effects were divided into two groups: local failure effects and plant failure effects.

Local Effects - the effect that an assumed failure mode has on the operation and function of the reactor trip and ESF protection system. It is possible for the local effect to be the failure mode itself.

Plant Effects - the total effect that an assumed failure mode has on the operation, function, or status of the plant or equipment other than the process protection system itself. The end effect may be the result of a double failure.

The list of potential plant failure effects for the process protection include:

| |
|------------------------------|
| PLANT FAILURE EFFECTS |
|------------------------------|

- *causes spurious reactor trip*
- *fails system X - wrong output*
- *fails system X - no response (fails as is)*
- *fails redundant train X-A only - system is functional -train generates wrong output*
- *fails redundant train X-A only - system is functional -no response (fails as is)*
- *causes spurious component (specify component if possible) actuation (change of state) - specify fail safe or not*
- *other - (explain). Add to this if applies to more than one case/component.*

E. Detection and Mitigating Features

Mitigating features include the actions, provisions and features that are available to prevent, negate, or mitigate the effects of a failure or correct the cause of failure. The intent is to identify those features which improve the current RPS over the previous RPS. Thus design, process, procedure and material changes are identified as well as existing design, process and material features that eliminate or mitigate the effects of a failure.

Westinghouse Non-Proprietary Class 3

Table 4-1 List I&C Components and Their Failure Modes

(This information will be enhanced upon design completion)

| Component | Failure Modes | Failure Causes | |
|----------------------------------|----------------------|-----------------------|--|
| DHC | | | |
| DLC | | | |
| I/O | | | |
| Processor | | | |
| Fiber Optic Transceiver (E/O) | | | |
| Fiber Optic Safety Net | | | |
| Fiber Optic Data Link | | | |
| Concentrators | | | |
| | | | |

4.2 FMEA Models

For this project, the FMEA models are created for the I&C upgrade system for the Kewaunee Nuclear Power Plant. Potential FMEA coverage can be in the following areas:

1. Reactor trip and ESF protection system;
2. ATWS mitigation and diverse actuation circuitry;
3. Fiber Optic Safety Net and non-class 1E workstation and bridge. (This is a non-safety system which is included to investigate if it creates undesirable system interactions with the other two systems listed previously.)

Example of an I&C FMEA is provided in Figure 4-2.

Figure 4-2 Failure Modes and Effects Analysis (an illustration)

| Component/ Assembly | Function | Failure Mode and Cause | Local Failure Effect | Plant Failure Effect | Detection and Mitigation |
|--------------------------------|--|---|--|----------------------|--|
| Input/Output subsystem: output | Provide interface between field-mounted equipment & E3 | Does not receive /transmit signals due to possible signal conditioning (A/D converter) on the board. | Loss of signals on a loop | No Effect | Man Machine Interface (MMI) Surveillance; Card replacement within required 8 hour repair time. |
| DLH Card (MMI Interface) | <ol style="list-style-type: none"> 1. Receives data from the tester DLH board. 2. Sends data from MMIP board to the tester DLH board. 3. Functions as a MULTIBUS slave. | <ol style="list-style-type: none"> 1.1 Fails to receive tester DLH data due to board component failure (dual-port RAM, EPROM, CPU, asynchronous duplex data link failure). | <ol style="list-style-type: none"> 1.1 No/bad data received from tester DLH (Loss of MMI functions) | No Effect | Man Machine Interface (MMI) Surveillance; Card replacement within required 8 hour repair time. |
| | | <ol style="list-style-type: none"> 2.1 Fails to send data from MMIP to DLH due to board component failure (EPROM, MPSC, CPU, asynchronous data link failure). | <ol style="list-style-type: none"> 1.1 Fails to send data from MMI to DLH (Loss of MMI functions) | No Effect | Man Machine Interface (MMI) Surveillance; Card replacement within required 8 hour repair time. |
| | | <ol style="list-style-type: none"> 1.1 Fails to maintain proper MULTIBUS slave interfacing due to board component failure (CPU, loss of 110 VAC, pulled card). | <ol style="list-style-type: none"> 1.1 Loss of MMI functions | No Effect | Man Machine Interface (MMI) Surveillance; Card replacement within required 8 hour repair time. |
| | | | | | |

5.0 DATA BANK CONSTRUCTION

In this section, a data bank for FTA is compiled. For this purpose, the following process is used:

1. The basic event data from Reference 1 is used whenever applicable. See Table 5-1 for this data.
2. For digital processing equipment (cards), available data from operating systems is used whenever available (Reference 3).
3. Otherwise, generic data is used (Reference 4).

This has been taken from a previous analysis that utilized historical data and parts count failure rates for similar equipment. It is recognized that this data is most likely conservative and can be scrutinized more closely upon stabilization of the equipment designs.

5.1 Data Used

Later

Table 5-1 Data Bank

| Failure Mode (Component) | Median | Error Factor [a] | Lognormal Distribution Mean and Interval [b] |
|--|---------|------------------|--|
| Channel Parameter Monitoring Instruments | | | |
| Pressure sensor/transmitter (CPR) | 6.9E-05 | 5.3 | (1.3E-05, 1.2E-04, 3.7E-04) |
| Temperature sensor/transmitter (CTP) | 5.6E-04 | 1.8 | (3.1E-04, 6.0E-04, 1.0E-03) |
| Eagle 21 processor (C21) [c] | 4.9E-06 | 5.3 | (9.2E-07, 8.2E-06, 2.6E-05) |
| Pressure processing module (CCP) | 8.2E-05 | 6.6 | (1.2E-05, 1.6E-04, 5.4E-04) |
| AT processing mod (CDT) | 4.0E-03 | 2.7 | (1.5E-03, 4.8E-03, 1.1E-02) |
| Processing module (CCX) | 6.8E-04 | 2.4 | (2.8E-04, 7.8E-04, 1.6E-03) |
| Bistable (CBI) | 3.9E-04 | 6.5 | (6.0E-05, 7.5E-04, 2.5E-03) |
| Trains (Trip Logic) | | | |
| SSPS universal card (TLC) | 1.4E-04 | 10.2 | (1.4E-05, 3.8E-04, 1.4E-03) |
| Bistable relay; undervoltage driver card relay (TLR) | 3.1E-05 | 3.0 | (1.0E-05, 3.9E-05, 9.5E-05) |
| SPSS undervoltage driver card (UVL) | 2.8E-04 | 2.6 | (1.1E-04, 3.4E-04, 7.4E-04) |
| Reactor Trip Breakers | | | |
| Breaker (mechanical/electrical) (BME) | 2.1E-05 | 5.6 | (3.8E-06, 3.7E-05, 1.2E-04) |
| RTB shunt trip device (BSN) | 4.5E-04 | 3.3 | (1.4E-04, 5.8E-04, 1.5E-03) |
| Control Rod Drive and Rod | | | |
| RTB undervoltage coil (BUV) | 2.1E-04 | 2.6 | (8.3E-05, 2.5E-04, 5.6E-04) |
| RCCA/CRDM (RMA) | 1.0E-05 | 4.0 | (2.6E-06, 1.5E-05, 4.1E-05) |
| a. Lognormal error factor corresponds to 5% and 95% bounds. | | | |
| b. Mean and lognormal distribution 5 th % and 95 th percentiles. Obtained by matching the mean and the variance of the distributions from Table C-7 of NUREG/CR-5500 Volume 2. | | | |
| c. Failure rate per hour, rather than probability of failure. | | | |

6.0 REACTOR TRIP FAILURE PROBABILITY

The system failure probability for reactor trip is modeled and quantified by using FTA in this section. As discussed previously in Section 3, the FTA model uses Reference 1 methodology and data as much as possible. The summary of the FTA analysis, as described in Reference 1 is provided next in Section 6.1.

6.1 RPS Modeling Standard from NUREG/CR-5500 (Based on a 4-loop Westinghouse PWR)

*This study documents an analysis of the operational experience of the Westinghouse RPS from 1984 through 1995. The analysis focused on the ability of the RPS to automatically shut down the reactor given a plant upset condition requiring a reactor trip while the plant is at full power. The term "reactor trip" refers to a rapid insertion of control rods into the reactor core to inhibit the nuclear reaction. RPS spurious reactor trips or component failures not affecting the automatic shutdown function were **not** considered. A Westinghouse RPS description is provided, followed by a description of the RPS fault tree used in the study. The section concludes with a description of the data collection, characterization, and analysis.*

6.2 FTA Assumptions

This section presents the assumptions, boundary conditions, and logic models used for quantification of system performance under various conditions. Each model depicts the system, given an initiating event.

Assumptions

1. Components analyzed for a reactor trip function include the sensors/detectors through the reactor trip and bypass breakers.
2. The analysis considers common mode failure as defined in Reference 1.
3. Multiplexing, alarm, and other status monitoring elements are not considered in the analysis conducted as they are isolated from the portions of the protective circuitry that perform reactor trip and safeguards actuation functions.
4. Wiring faults are not considered in the analysis conducted. It is assumed that occurrence

of open circuits is negligibly small and that occurrence of short circuits is insignificant.

5. Two types of reactor trip models are developed; one with functional diversity, for Condition II and III events (the base case), and one for Condition IV events with no consideration of diversity (as a sensitivity case). Since Condition II and III events are expected to be more frequent than those of Condition IV events, signal diversity would increase system actuation reliability.

A representative accident for Conditions II and III is chosen to be a Loss of Normal Feedwater, since it is a frequent transient initiator. The typical signals modeled are low-low steam generator water level and high pressurizer pressure, as they represent the primary and a backup protection signal for the chosen representative accident. Since all Condition II and III accidents are protected by at least two diverse reactor trip signals, and the diverse parameters are "ANDed" in the system fault tree, the specific choice of signals is not important. Any two reactor trip signals could be chosen and would yield similar results. This reactor trip fault tree is applicable to all Condition II and III accident initiators.

6.3 Fault Tree Top Logic

The RPS fault tree top logic is generated from the new I&C system diagram given in Figure 2-1. The block diagram for the top logic is as follows:

| | |
|------------------------------|------|
| Process sensors | SENS |
| Process Protection Cabinets | PPC |
| Fibre Optics Data Links | FODL |
| Voting Logic Cards | VLC |
| Dynamic Trip Buses | DTB |
| Reactor Trip Breakers | RTB |
| Control Rod Drive Mechanisms | CRDM |

The following table compares this block diagram with that of NUREG/CR-5500 logic for Eagle 21:

| New I&C | Eagle 21 |
|--------------------|-----------------|
| Process Sensors | Sensors |

Westinghouse Non-Proprietary Class 3

| | | | |
|------------------------------------|-------------|---|------|
| Process Protection Cabinets | PPC | Process Logic Modules Output Bistables TMU Relays | |
| Fibre Optics Data Links | FODL | ---- | |
| Voting Logic Cards | VLC | Solid State Logic | SSL |
| Dynamic Trip Buses | DTB | Solid State Logic | SSL |
| Reactor Trip Breakers | RTB | Reactor Trip Breakers | RTB |
| Rod Control Cluster Assemblies | RCCA | Rod Control Cluster Assemblies | RCCA |

The different subsystems in the new I&C design (PPC, FODL, VLC, and DTB) are shown in bold letters.

6.4 Fault Tree Model

Later

7.0 ENGINEERED SAFEGUARDS ACTUATION FAILURE PROBABILITY

In this section, a quantitative analysis of ESFAS reliability is performed by using a fault tree model.

7.1 FTA Assumptions

A representative ESFAS model is developed for the generation of an SI signal on low pressurizer pressure. The representative unavailability is conservatively applicable to each of the safeguards actuation functions listed below:

- Safety Injection Signal
- Auxiliary Feedwater Pump Start
- Containment Isolation
- Containment Ventilation Isolation
- Steamline Isolation
- Feedwater Isolation
- Containment Spray

125 VDC instrumentation power is modeled within the ESFAS fault tree. Power is necessary for the load sequence relays, master relays, and the slave relays that must energize to actuate their loads.

120 VAC instrument power on 4 instrument buses (red, white, blue, and yellow) is also supplied.

Components analyzed for an EFS actuation function include the sensors/detectors through the master relay coils and contacts. Slave relays and auxiliary master and slave relays and time delay relays should be included in the specific EFS components which they actuate.

7.2 FTA Top Logic

Later

7.3 Fault Tree Model

Later

8.0 SENSITIVITY ANALYSES

No mathematical uncertainty analysis is performed in this study. However, sensitivity analyses to provide insights into the various assumptions, parameters, and configurations of the system are given in this section. Effect of manual actuation credit is already discussed in the base case FTA models.

The following cases are analyzed:

1. Reactor trip without diverse actuation signals.

A LOCA is chosen as the representative Condition IV accident and the typical reactor trip signal is low pressurizer pressure, since it may be the only reactor trip signal received in the event of a very small LOCA. This reactor trip fault tree must be used for all Condition IV accident initiators in the absence of functional diversity for reactor trip.

2. Effect of AMSAC on RPS reliability.
3. Allowable software error probability.
4. Later

8.1 Reactor Trip Without Diverse Actuation Signals

Later

8.2 Effect Of AMSAC On System Reliability

9.0 SUMMARY, CONCLUSIONS, AND INSIGHTS

LATER

10.0 REFERENCES

1. NUREG/CR-5500, Vol.2 : Reliability Study: Westinghouse Reactor Protection System, 1984-1995, April 1999.
2. ANSI/IEEE Std. 352-1987, "IEEE Guide For General Principles Of Reliability Analysis Of Nuclear Power Generating Station Safety Systems".
3. Data Reference - Later
4. Data Reference - Later
5. Updated Final Safety Analysis Report, Kewaunee Nuclear Power Plant, Wisconsin Public Service Corporation, Rev. 15, 1999. (Revision 16 expected in Jan/Feb. 2000)
6. Kewaunee Nuclear Power Plant Reactor Protection System Upgrade Project, June, 1999 Kewaunee letter number NRC-99-041.