Westinghouse
Electric Company LLC

Box 355
Pittsburgh Pennsylvania 15230-0355

WCAP-15413 Rev. 0
Project Number 694

WOG-ASIC-00-024
June 21, 2000

Document Control Desk
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Attention: Chief, Planning Program and Management Support Branch

Subject: Westinghouse Owners Group
ASIC Subgroup
Submittal of Application Specific Integrated Circuit (ASIC) Licensing Summary Report (MUHP-7300)

Reference:
1) OG-97-069, dated July 10, 1997
2) WOG-ASIC-98-002, dated June 5, 1998
3) WOG-ASIC-99-019, dated August 9, 1999
4) WOG-ASIC-00-004, dated January 27, 2000
5) WOG-ASIC-00-005, dated February 7, 2000
6) WOG-ASIC-00-007, dated March 6, 2000
7) WOG-ASIC-00-019, dated May 9, 2000

Enclosed are three (3) copies of the "Westinghouse 7300A ASIC-Based Replacement Module Licensing Summary Report": WCAP-15413, Rev. 0 (Westinghouse Non-Proprietary Class 3), dated May 2000.

Application Specific Integrated Circuit (ASIC) technology is a state-of-the art technology that addresses the issues encountered by "Vintage Instrumentation and Control" (I&C) equipment life cycle management programs. The focus of the ASIC program was to design an ASIC-Based Replacement Module (ABRM) for a Westinghouse(W) supplied 7300 Process Protection System or Process Control System, that could be implemented at individual plant sites under 10 CFR 50.59 without prior NRC approval. The ASIC-based replacement card is intended to be a spare part and a card for card replacement for specific 7300 analog cards in operating plants.

The information contained in the attached non-proprietary summary report along with the proprietary information previously submitted and referenced meets the requirements of 10 CFR Section 2.790 of the Commission's regulations requiring submittal of both proprietary and non-proprietary versions on the ASIC licensing topical report once it is completed. Since a proprietary summary report would consist only of a compilation of the previously submitted proprietary information, referenced above, a proprietary summary report is not being issued.

It is the purpose of this report, as supplemented by the previous submittals and reports, to provide the NRC with sufficient information to conclude that implementation of ASIC-based replacement cards does not result in an unreviewed safety question.

Submittal of this report completes the documentation to be presented to the NRC in support of the ASIC-Based replacement cards.

NRR-102

D048 1/3

Invoices associated with the review of this WCAP should be addressed to:

Mr. Andrew P. Drake, Project Manager
Westinghouse Owners Group
Westinghouse Electric Company
(Mail Stop ECE 5-16)
P.O. Box 355
Pittsburgh, PA 15230-0355.

Please direct any questions or comments regarding the information in this submittal to Mr. Richard (Dick) B. Miller of Westinghouse at (412) 374-5953.

Very truly yours,

Michael G. Eidson, Chairman
ASIC Subgroup
Westinghouse Owners Group

Enclosure (3 copies)

cc: ASIC Subgroup Representatives (1L, 1E)
WOG Steering Committee (1L)
Eric J. Lee, USNRC (1L, 1E)
Stephen D. Bloom, USNRC (1L, 1E)
A. P. Drake, W - ECE 5-16 (1L)

Westinghouse Non-Proprietary Class 3

WCAP - 15413
Revision 0

Westinghouse 7300A ASIC-Based Replacement Module Licensing Summary Report

Westinghouse Electric Company LLC

WCAP-15413

Westinghouse 7300A ASIC-Based Replacement Module Licensing Summary Report

C. A. Vitalbo
I&C Projects and Operations

R. B. Miller
Regulatory and Licensing Engineering

May 2000

Approved: S. Radomski, Manager
I&C Projects and Operations

Westinghouse Electric Company LLC
P.O. Box 355
Pittsburgh, PA 15230-0355

©2000 Westinghouse Electric Company LLC
All Rights Reserved

RECORD OF REVISIONS

WCAP-15413

Rev. No.	Date	Author	Description
0	5/2000	C. A. Vitalbo/R. B. Miller	Original Issue

Westinghouse Electric Company LLC
P.O. Box 355
Pittsburgh, PA 15230-0355

©2000 Westinghouse Electric Company LLC
All Rights Reserved

ACKNOWLEDGMENTS

The following utilities are acknowledged for their contributions to this program in the areas of design reviews, documentation reviews, module testing, general guidance and meeting support.

Commonwealth Edison

First Energy Nuclear Operating Company

Northeast Utilities

South Carolina Electric & Gas

Southern Nuclear Operating Company

STP Nuclear Operating Company

Virginia Power Company

Wolf Creek Nuclear Operating Company

TABLE OF CONTENTS

1.0 INTRODUCTION 1-1

2.0 SYSTEM DESIGN DESCRIPTION 2-1

3.0 DESIGN, VERIFICATION & VALIDATION PROCESS 3-1

4.0 ASIC CHIP TEST RESULTS 4-1

5.0 VALIDATION TEST PROGRAM 5-1

6.0 QUALIFICATION TESTING 6-1

7.0 RELIABILITY ASSESSMENT & FMEA RESULTS 7-1

8.0 WESTINGHOUSE SAFETY EVALUATION 8-1

9.0 SUPPLEMENTAL REPORT ON RESPONSE TIME TEST DELETION 9-1

10.0 REGULATORY CRITERIA COMPLIANCE 10-1

LIST OF TABLES

Table 2-1 7300 MODULE OUTPUT VOLTAGE REQUIREMENTS 2-3

Table 4-1 FAULT ANALYSIS SUMMARY 4-10

Table 9-1 ARBM RESULTS/ANALOG COMPARISON 9-6

LIST OF FIGURES

Figure 2-1 ABRM BLOCK DIAGRAM 2-19

Figure 2-2 ABRM OPERATOR INTERFACE 2-20

Figure 2-3 ABRM CONTROLLER 2-21

Figure 2-4 ABRM ALARM CIRCUIT LOGIC 2-22

Figure 4-1 NOR GATE PRIMITIVE CELL 4-18

Figure 4-2 ASIC FUNCTIONAL BLOCK DIAGRAM 4-19

1.0 INTRODUCTION

Application Specific Integrated Circuit (ASIC) technology is a state-of-the art technology that addresses the issues encountered by "Vintage Instrumentation and Control" (I&C) equipment life cycle management programs. For a Westinghouse (W) supplied 7300 Process Protection System or Process Control System, the ASIC technology will be implemented as a card-for-card replacement.

The focus of this program was to design an ASIC-Based Replacement Module (ABRM) which is a card-for-card replacement module that can be implemented under 10 CFR 50.59, requiring no prior approval from the NRC. The ASIC-based replacement card is intended to be treated as a spare part for specific 7300 analog cards in operating plants.

1.1 REQUEST FOR NRC REVIEW AND APPROVAL

The WOG is submitting this topical report to the NRC for review and approval in order to implement ABRMs in the 7300 Process Protection and Control System under 10 CFR 50.59 at individual plant sites. It is the purpose of this report to provide the NRC with sufficient information to conclude that implementation of ASIC-based replacement cards does not result in an unreviewed safety question.

1.2 DRIVING FACTORS FOR ASIC-BASED SOLUTION

There are several factors that drive the industry to an ASIC-based solution.

(1) The domestic reactors are operating with most of the original installed I&C systems. This technology is over 20 years old. Most utilities have significant operating experience with their current systems and are now faced with rising costs to maintain equipment. As the systems get older, the industry is faced with potential component obsolescence issues and increasing pressures to improve plant performance and availability.

(2) Utilities are resistant to make large-scale changes due to costs associated with impact on plant procedures, significant changes to the internal cabinet wiring, and outage schedules. Constraints for the ASIC-based module development program were to minimize impact on plant procedures, require no internal cabinet wiring changes, and to minimize impact on the current operator interface.

(3) Utilities have maintained large inventories of replacement parts, which is a significant annual cost (i.e., 20% - 30% of inventory value). The ABRM is a product that can be easily configured in the field to replace any one of 14 PPS and PCS cards, thus significantly reducing inventory requirements.

(4) Power dissipation (heat buildup) in the cabinets shortens module/card life. ASIC-based modules dissipate significantly less power, thus extending module life. In

addition, the ASIC-based modules have a higher design operating temperature, making them more resistant to heat induced failures.

(5) Obsolescence issues make it increasingly more difficult to procure replacement components. The ASIC chip itself is fabricated using the same technology used to manufacture today's integrated circuits (transistors, operational amplifiers, memories, logic devices, etc.). Thus, the ASIC device can be made as long as the technology exists to manufacture integrated circuits.

In summary, an ASIC-based replacement card reduces the economic risk associated with maintaining 20-30 year old I&C systems.

1.3 APPROACH

An industry alliance was formed between the Westinghouse Owner's Group (WOG) utilities, EPRI, and Westinghouse Electric to develop, license, manufacture, and demonstrate the ASIC-based replacement cards. The development program addressed the Westinghouse 7300 System hardware that was originally installed in the Westinghouse supplied process protection, control, and balance-of-plant (BOP) systems. The ASIC-based card design is a form, fit, and functional replacement that contains no software (programmable code).

The alliance defined a program that minimizes the impact on the plant procedures, system wiring, design basis, and licensing basis. The program objective was to design the replacement card to meet the current design and licensing basis requirements, allowing utilities to replace their analog cards with the ASIC-based cards under their current replacement part programs. The following elements of the development program strongly support this objective.

(1) The ASIC-based replacement card allows the utilities to maintain the mature system design and architecture. The replacement design is built on proven system performance. The system design basis is well known. The system licensing basis is well known. Both the design basis and licensing basis are preserved with the replacement cards. The replacement card can be inserted as an analog replacement card and therefore becomes a spare part.

(2) A program-specific design, verification, and validation plan was developed. This plan captured the Westinghouse robust design process and 10 CFR 50 Appendix B requirements. The design, verification, and validation process assures proper translation of functional and performance requirements, that the proper reviews have been performed, and that the devices have been exhaustively tested. This plan is presented in detail in Section 3 of this report.

(3) Vendor experience with respect to this replacement card is significant. Westinghouse is the OEM supplier of these systems and has written all documentation associated with the design and licensing of these systems. Northrop Grumman ATC is a supplier of military components used in safety critical applications. ATC has extensive experience in the design and application

of custom integrated circuit technology. ORNL is a National Lab and has extensive experience in the design of ASICs. ORNL, in conjunction with EPRI, developed a prototype ASIC for use in safety applications. This prototype served as a starting point for this application.

(4) End user involvement has been high throughout the various stages of the program. The end users have hundreds of years of operating experience with these systems. The design specifications were based on end user input. The end users have specified the requirements for the operator interface and test point requirements based on their current operating procedures. The high involvement of the utilities in this program significantly strengthens the vendor-utility interface.

(5) The design process included the provision for selection of highly reliable components. ASIC technology has a demonstrated reliability on the order of 1x10-7 failures per year. The design objective for the NXX Main Board was an MTBF greater than 100,000 hours. In general, components were selected to have higher performance requirements than their analog board counterparts.

(6) The ASIC-based replacement card is a hardware based versus software based replacement. Hardware is distinguished from software by the degree of testability. The ASIC-based card does not have the characteristics associated with microprocessor based systems such as modifiable code, branches or interrupts, decision making capability, lockups, and common mode software failure susceptibility. The ASIC-based card operation is deterministic and sequential and failures can be treated as single random hardware failures.

(7) Finally, the degree of testability of the design assures proper operation and confidence that no new failure modes have been created. Testability is obtained through the simplicity of the ASIC-based card design. The card is pin-for-pin compatible with the card it replaces and requires no cabinet wiring changes. The ASIC performs simple math functions that are easily tested. Process functions built from combinations of the ASIC math functions are thoroughly tested in the validation test program.

2.0 SYSTEM DESIGN DESCRIPTION

This section contains a detailed discussion of the principles and theory of operation of the ASIC-Based Replacement Module (ABRM). Figure 2-1 is a simplified functional block diagram depicting the approach for the 7300 System hardware. The text is separated into discussions of the Power Supply and Distribution circuits, Input and Output Signal Conditioning, Operator Interface, and the ASIC chip and Controller.

DESIGN CONSTRAINTS

The following design constraints were imposed by the Design Team.

(1) The ASIC-based replacement module must be pin-for-pin compatible with the module it replaces. In other words, implementation requires no internal cabinet wiring changes.

(2) The ASIC-based replacement module must have the same accuracy as the module it replaces.

(3) The design must be licensable for implementation under 10 CFR 50.59.

(4) The design shall not contain any software or programmable (modifiable) code.

(5) The ASIC design must be completely testable at the component (chip) level.

(6) The functionality of the replacement module will remain the same as the analog module it replaces.

(7) The design must be capable of reconfiguration to perform multiple functions.

(8) The board must be designed so that it can be inserted and removed while the cabinet (chassis) is energized.

(9) The design shall minimize impact on the current operator interface, i.e., setpoints and tuning constants entered as voltages with no hand-held devices.

(10) The design shall minimize impact on existing plant procedures and training.

(11) The design shall minimize impact on existing maintenance and test equipment.

(12) A design goal is to limit the input current requirement to 75% of the equivalent 7300 analog module to reduce internal cabinet heat dissipation.

(13) A design goal is to increase the maximum ambient operating temperature from 140 to 158 Degrees Fahrenheit (from 60 to 70 Degrees Celsius).

2.1 SCOPE

An ASIC-based replacement module will directly replace the following 7300 System analog modules.

7300 MODULE TYPE	PART NUMBER	DESCRIPTION
NAC	2838A32	Analog Comparator Card
NAL	2837A13	Signal Comparator Card
NCB	2838A30	Controller Card
NCD	2837A16	Controller Driver Card
NCH	2837A11	Function Generator Card
NLL	2837A18	Lead/Lag Amplifier Card
NLP	2837A12	Isolator & Loop Power Supply
NMA	2838A34	Mixing Amplifier Card
NMD	2837A19	Multiplier/Divider Card
NRA	2837A15	RTD Amplifier Card
NSA	2837A14	Summing Amplifier Card
NSA5 (MSS)	2837A14GO5	Median Signal Selector Card
NSC	2837A10	Signal Converter Card
NTD	2838A45	Tracking Driver Card
NVP	2837A21	Voltage-To-Pulse Converter

2.2 POWER SUPPLY AND DISTRIBUTION

The Power Supply and Distribution circuit receives nominal +26/26, +26/24, or +24/24 Volts DC from the 7300 cabinet main power supplies. Multiple on-board DC/DC converters provide all necessary DC power for the analog input and output signal conditioning circuitry, the digital actuation output circuitry, the Operator Interface and all local indicators. The output of DC/DC Converter 1 is +5 VDIG and is used for all of the digital input and output circuitry. DC/DC Converter 2 provides +5 V for the ASIC, Controller, Operator Interface, RAMLogic, contact inputs and alarm circuitry. A +2.5 VDC output is derived from the +5 V output, which is used for the analog input signal conditioning circuitry. DC/DC Converter 3 provides ±15 VDC, which is used for the Operator Interface, analog and digital output signal conditioning circuitry. Series regulators are used to derive ±5 VANALG, which is also used by the analog input signal conditioning circuitry. Isolated power is supplied by DC/DC Converter 4. The output voltages of ±15 VISO, +5 VISO and +2.5 VISO are used by the isolated analog output signal conditioning circuitry.

Various 7300 modules contain voltage outputs for use in different applications. These voltages are used to bias external potentiometers, apply bias voltages to input signals, etc. The voltage output requirements for the various 7300 modules are identified in Table 2-1.

TABLE 2-1

7300 MODULE OUTPUT VOLTAGE REQUIREMENTS

Output	NCB	NMD	NSC	NAL	NLP	NTD	NCD	NRA	NMA	NAC	Note
+10 V	X	X									PM
+20 V				X							PM
–20 V				X							PM
+40 V					X						PM
+60 V					X						PM
2 mA								X			PM
+5 V							X				MB
+10 V Bias									X		MB
+26/ +24 V			X	X			X			X	MB

In order to supply all of the various voltages required for the different 7300 card styles and conserve real estate on the Main Board, the Personality Modules for the respective card styles are designed with on-board power supplies. For example, the NRA Personality Module contains the 2 mA RTD excitation current circuit. The "MB" designation in the Note column signifies that the output voltage requirement for those card styles is derived from the Main Board (instead of the PM) and routed to the proper output pin via the Personality Module. The variable +10 V bias voltage is derived from analog output channels 5 and 6. The +26/24 V auctioneered voltage is derived from the Main Board. Test points are available to check each voltage output.

In RTD applications, the NRA Personality Module provides a precise 2 milliamp RTD excitation current source. With a constant current, the voltage developed across the RTD is directly proportional to the change in the RTD resistance, which is proportional to the measured temperature. The measured voltage is used by the ASIC chip to calculate the RTD resistance and respective process temperature. Typical design accuracy for the precision RTD constant current source is 0.1 %.

In loop power supply applications, the Main Board provides the +40 VDC necessary to power field mounted transmitters. The transmitter functions as a current regulator, varying the loop current from 4 to 20 mA over its calibrated range with respect to the process variable being measured (pressure, level, flow, etc.). The current flow produces 1-5 VDC across a 250 ohm resistor in the input signal conditioning circuit located on the NLP Personality Module. Since

the transmitter regulates the current, the voltage source accuracy is approximately ±2.5 %. The design also contains provisions to series-connect the power supplies to form a single +60 VDC power source. This is used to power transmitters with 60 VDC requirements (10-50 mA interface). In addition, the voltage outputs (+40 VDC or +60 VDC) can be used for external contact wetting voltage if so desired.

The +26 VDC and +24 VDC input voltages from the cabinet power supplies are diode auctioneered and fuse-protected on the Main Board. The auctioneered voltage is provided to one of the output pins. This auctioneered voltage can be used to:

(1) Power the voting logic relay coils for NAC and NAL applications;

(2) Power the Manual/Auto (M/A) station indicators and push-buttons; and

(3) Provide external contact wetting voltage.

2.3 INPUT SIGNAL CONDITIONING

The input signal conditioning circuitry is contained on the Main Board, and it performs the signal conditioning, process noise filtering, calibration and analog-to-digital conversion (ADC) functions. There are 4 identical, independent channels of input signal conditioning, and provisions to add another 4 input channels. Each channel receives input voltage(s) from the Personality Module, filters the signal to remove process noise, and performs the analog-to-digital conversion. The Personality Modules are designed to accommodate their respective input signal types, so that the interface to the Main Board input channel is the same.

In addition to 8 analog inputs, the ASIC-based module is designed to process up to 8 contact inputs. This is accomplished by switching the 8 analog serial input busses into an 8-bit parallel input bus during the read cycle. This feature provides the capability to interface with a 7300 M/A Station, or other external contact inputs. Contact wetting voltage can be provided by either the auctioneered +26/+24 VDC output or by using the voltages available from the PM.

The buffer/process noise filter amplifier circuit converts the differential input signal into a single-ended signal. A low-pass process noise filter in the ADC eliminates unwanted process noise above 10 Hz. The ADC provides the interface to the ASIC, and it has an effective resolution of 15 bits.

Calibration of the analog input signal conditioning circuitry is automatic via self-calibrating ADCs. Upon power-up, the ADCs automatically calibrate over their full range of operation. The calibration routine can be manually initiated by the operator via the Operator Interface. Input calibration is separate and independent from the output calibration. This facilitates use of root-mean-square (RMS) accuracy calculations.

2.4 ANALOG OUTPUT SIGNAL CONDITIONING

The analog output signal conditioning circuitry contained on the Main Board performs the digital-to-analog conversion (DAC), signal conditioning, filtering, calibration, isolation and surge protection functions. The Main Board contains one ±10VDC voltage output and one 4-20 mA current output. The voltage output can be isolated for NLP applications, and the current output can be isolated for NSC applications. Additional outputs, if required by the application, are generated by the respective Personality Module. Up to 5 additional voltage outputs can be generated.

The parallel output of the ASIC is converted into serial data by the parallel-to-serial converter that is part of the RAM Logic field programmable gate array (FPGA). The serial data is optically coupled to the DACs for isolation. This approach does not require transformers and is necessary to achieve the required through-put accuracy as well as functionality. The DACs are 16 bit devices, and they generate an output signal range of –10/+10 or 0-10 VDC. Effective resolution is 15 bits.

The buffer/process noise filter amplifier receives input from the DACs, filters high-frequency noise from the signal, and generates the differential output signals. The –10/+10 or 0-10 VDC isolated differential output can supply an output load impedance greater than 600 ohms. The 4-20 mA isolated differential output can supply a maximum load of 1250 ohms. The outputs are short/open circuit protected.

Calibration of the output signal conditioning circuitry is performed by gain and offset potentiometers located on the Main Board. Output calibration is separate and independent from the input calibration. This facilitates use of root-mean-square (RMS) accuracy calculations.

2.5 DIGITAL ACTUATION OUTPUT SIGNAL CONDITIONING

The digital actuation output circuitry is contained on the NAC and NAL Personality Modules, and it generates the on/off control function to the protection logic relays. There are 4 independent channels of digital actuation output signal conditioning, each with the following capabilities:

a. 250 mA sink capability;

b. Complementary logic output pairs;

c. Short circuit protection;

d. LED indication on "sink-side" outputs;

e. Isolation; and

f. Normally Energized (NE) or Normally De-energized (ND) outputs.

The digital actuation output channels are driven by steady-state high/low logic level signals from the ASIC. In the normal (non-tripped) condition, the ASIC comparator output is a steady-

state low signal. When the ASIC comparator calculates a partial trip, the output will go high, causing the external output to change state. Red LED indicators on the front edge of the NAC and NAL PMs provide local indication of the status of the "sink side" outputs. When the NE or ND sink output is conducting, the LED indicator will be illuminated. The digital actuation outputs can also be used to illuminate the 7300 Series M/A station push-button indicators for raise, lower, upper/lower limit, etc.

2.6 OPERATOR INTERFACE

Refer to Figure 2-2. The Operator Interface (OI) circuitry provides the means by which the process function setpoints and tuning constants are entered, stored and changed. The OI is designed to emulate as close as possible the current method of entering and changing setpoints and tuning constants. This means that all setpoints and tuning constants are entered as voltages instead of numerical values.

The OI design consists of logic and memory circuitry located on the Main Board, and card-edge mounted components. Features of the OI design are as follows:

- Stores up to 100 setpoints and tuning constants;
- Up/Down Switch used in conjunction with a push-button and digital voltmeter (DVM) to enter/change calibration values;
- Maintains existing scaling methodology (volts represent engineering units);
- Non-Volatile Memory does not require battery backup for retention capability;
- Setpoints and Tuning Constants can be changed on-line; and
- All components accessible from front of card (does not require removal).

Figure 2-2 depicts the OI design. When the Selector Switch is in the "0" (OFF) position, the OI circuitry is de-energized to minimize power consumption and prevent accidental setpoint changes. When the Selector Switch is placed in the "1" (Select/Read Tuning Constant Index/Tuning Constant Value) position, the OI circuitry is energized. The 2 digit numerical display indicates "88" to test all 7 segments of the display and the DVM connected to the TEST POINT will read "5.000" volts. With the Selector Switch in the "1" position, manipulation of the Up/Down Switch causes the up/down counter to sequence to the desired tuning constant index for storing a tuning constant value. There are 100 memory locations, from "00" to "99". When the desired TCI is obtained on the display, the DVM will read the voltage representing the stored tuning constant value. When the Selector Switch is rotated to the "2" (Set TCV) position, the Up/Down Switch is used to set/change the scaling voltage representative of the desired setpoint or tuning constant. The voltage setting accuracy is 1.0 millivolt DC. Holding the Up/Down Switch for more than 2 seconds will cause the rate of change to increase. When the desired setting is obtained, the push-button is depressed. This will lock the digital value representing the analog voltage into the memory location selected earlier. The process is

repeated until all setpoints and tuning constants are entered. Upon completion, the Selector Switch is returned to the "0" position, and the OI circuitry is de-energized.

The ASIC accesses the setpoints and tuning constants each cycle. The setpoints and tuning constants are stored in two locations, EEPROM and Dual Port RAM (DPRAM). The EEPROM stores the values set by the I&C technician. The DPRAM contains an exact copy of the values stored in EEPROM. Each cycle, the ASIC accesses and uses the values stored in DPRAM. When the ASIC releases control of DPRAM (i.e., a NO-OPS signal), the OI can update the DPRAM values from EEPROM. This approach allows for on-line changing of setpoints and tuning constants without corrupting the on-going process, and it provides backup storage in case of power loss. The EEPROM does not require battery backup.

Placing the Selector Switch in position "9" (CAL_ADC) will initiate automatic calibration of the input signal conditioning circuitry. The input calibration will result in an input accuracy of approximately 0.04 %.

Selector Switch positions "8" (DAC_Offset) and "7" (DAC_Gain) are used to calibrate the OI DAC and the 2 DACs used in the analog output circuitry (1 on the Main Board and 1 on a PM). There are 2 potentiometers for each DAC, one for offset and one for gain, resulting in a total of 4 potentiometers on the Main Board and 2 potentiometers on a PM. Placing the Selector Switch in position "8" will enable manual zero-offset adjustment of the 3 DACs. Placing the Selector Switch in position "7" will enable manual gain-offset adjustment of the DACs. The output calibration will result in an output accuracy of approximately 0.05%.

With self-calibrating ADCs and manual gain and offset adjustment of the DACs, the resultant overall through-put accuracy of the ASIC-based replacement module is 0.1 %. The Main Board and Personality Modules are calibrated during factory acceptance testing.

Selector Switch positions 3 (FSH), 4 (Zero) and 5 (FSL) are used to facilitate entry of TCVs of +10 VDC, 0 VDC, and –10 VDC respectively.

2.7 ASIC CHIP

The ASIC-based replacement module design approach is to design one ASIC chip that can be used for all applications. The ASIC chip is mounted on the Main Board that fits into the existing card frame, making external wiring changes unnecessary.

2.7.1 Background

An ASIC prototype using field programmable gate arrays (FPGAs) was built by Oak Ridge National Lab as part of a Cooperative Research and Development Agreement (CRADA) jointly funded by the Department of Energy and the Electric Power Research Institute. Work done under the CRADA was used to develop a method of approach (mathematical functions) and to design and build prototype equipment that demonstrates ASICs technology in safety system applications. The prototype equipment demonstrated the capabilities, features, and design methods of ASICs. The prototype equipment, built under the CRADA, implemented the

relatively simple pressurizer pressure protection channel and the more complex over-power and over-temperature protection channel functions used in the Westinghouse designed process protection system. The prototype implements these safety functions by combining simple mathematical functional modules to perform more complex process functions. This work showed that a relatively simple ASIC device can be used to implement safety system functions. It demonstrated the feasibility of the ASIC technology and of the concept.

During the conceptual design phase, two options for the architecture of the ASIC module were proposed to the WOG Core Group. The first option was to implement standard math functions in the ASIC, based on the prototype work performed by ORNL. The standard math functions are: add, subtract, multiply, divide, square root, compare and function generator. A Controller PROM would be designed to enable the standard math functions in the correct sequence to perform a process function, such as lead/lag. The second option was to implement the process functions in the ASIC. The process functions are: summator, multiplier, divider, square root, comparator, lead/lag, function generator, PID and median signal selector. The final decision to design the ASIC chip based on mathematical functions was based on the following:

- Mathematical functions are standard, simple, and well understood;
- Simple math functions can be thoroughly tested;
- Math-based functions provide more flexibility than process based functions, i.e., allows future implementation of other process-based functions;
- Math-based functions required less gates than process-based functions; and
- Process functions would increase chip size and therefore price.

2.7.2 ASIC Chip Design

The ASIC chip contains sets of individual circuits. Each individual circuit performs a basic math or interface operation. The basic math circuits perform computations that can be combined to perform higher level process functions. In some cases the higher level function is the same as the basic computation in the ASIC, such as that done for addition. The individual math-based circuits in the ASIC are add/subtract, multiply/divide, compare, square root, ADC control, DAC control, storage registers, and controller/counter. Each circuit has an enable code that controls its operation. An external controller, stepped by the ASIC counter, contains the enable codes for the ASIC circuits. Eight internal registers are used to store intermediate values for process computations, but if there are not enough internal registers for a process computation, external RAM can be used to store temporary or intermediate values.

The ASIC design uses fixed point math to avoid the complexities of floating point computations. Numbers in the ASIC are represented as binary with 16 bits left of the decimal point and 23 bits right of the decimal point. The largest decimal numbers that can be represented are ± 65,536 with resolution equal to 0.12E-6. The ASIC represents numbers in sign-magnitude format. Bit 39 is the sign, and bits 0 through 38 are the magnitude.

DIAGNOSTICS, CONTROLLED FAILURES, AND ERROR FLAGS

A limited amount of diagnostics are included in the ASIC design to assist operators in identifying a failed channel. The diagnostics are not used to prevent misoperation of the ASIC. The diagnostics include error flags for overflow by addition, subtraction, multiplication, and division (including division by zero). The diagnostics include a controlled failure mode such that if an overflow occurs, the magnitude of the output is set to maximum and the sign is set appropriate to the input numbers. The output is set to maximum after an overflow to control the failure because it is possible for an overflow to result in a value that is near nominal value. In some cases, the maximum value will result in a channel trip, but not for all cases. An error flag is also set if a significant bit is shifted left out of the shift register during a shift-left operation. In the event one of these errors occurs, the error flag is set and the ASIC continues without interruption. The ASIC is not halted for an error because it is possible that the error occurred because of a transient. If the error resulted from a transient, the output will return to normal during the next cycle. It is also possible that the error flag occurred because of a permanent hardware failure, in which case the error flag would remain on. The operators can use the error flag to find the failed channel. There are failures that will not be detected by these limited diagnostics, but flags and the controlled failure modes provide some assistance in detecting a failure without creating a nuisance alarm scenario. The purpose of the error flags are to help operators detect a failed channel, not to prevent the card from outputting a wrong value.

ADD FUNCTION

The add circuit performs signed addition or subtraction of two numbers. It also does two's complement, shift right, shift left, and absolute value on a single number. Scaling the numbers to be 0 to 10 V, the systematic full scale error of the result of addition or subtraction is 2.4E-6 %. There is no systematic error for shift, magnitude, or two's complement. Each of the functions in the add circuit are done in one clock cycle. The resultant can be loaded into any of the eight storage registers.

In case of overflow for addition, the output magnitude is set to maximum, the sign is kept appropriate for the sum, and an error flag is set. If a significant bit is lost for shift left, an error flag is set. Calculations are not stopped in case of an error flag.

MULTIPLY FUNCTION

The multiply circuit performs a signed multiplication of two numbers. Multiplication of two 40-bit numbers results in an eighty bit number that is rounded to a 40-bit number. Scaling the numbers to be 0 to 10 V, the systematic full scale error of the result of multiplication is 2.4E-6 %. The resultant can be loaded into any of the eight storage registers.

In case of overflow, the multiplier resultant is set to maximum magnitude, the sign is set appropriate for the two inputs, and an error flag is set. Calculations are not stopped in case of an error flag.

DIVIDE FUNCTION

The divide circuit performs a signed division of two numbers. The division is carried out to retain 40 bits in the resultant. Scaling the numbers to be 0 to 10 V, the systematic full scale error of the result of division is 2.4E-6 %. The resultant can be loaded into any of the eight storage registers.

In case of overflow or division by zero, the resultant is set to maximum magnitude, the sign is set appropriate for the two inputs, and an error flag is set. Calculations are not stopped in case of an error flag.

SQUARE ROOT FUNCTION

The square root circuit performs the square root of a positive number. The square root is carried out to retain 40 bits in the resultant. Scaling the numbers to be 0 to 10 V, the systematic full scale error of the result of square root is 0.6E-6 %. The resultant can be loaded into any of the eight storage registers.

In the case of square root of a negative number, the resultant is set to the value of the root of the positive number, the sign is set to positive, and an error flag is set. Calculations are not stopped in case of an error flag.

COMPARATOR FUNCTION

The comparator can perform many different types of comparisons. The comparator circuit performs the following functions: window mask, which is used in the function generator; compare A to B and output the largest; compare A to B and output the smallest; and window compare with true/false output (i.e., $A>B$, $A=B$, $A<B$, $A \leq B$ and $A \geq B$). There are no systematic errors in the comparison circuits. Each comparison takes one clock cycle.

A window compare is used to detect a value between two set points. The comparator includes a feature for hysteresis by having the trip output(s) selecting whether to compare input A to set point B, the normal trip point, or to set point C, which is the hysteresis set point.

There are eight trip outputs from the ASIC. Any of the trip outputs can be logic level or pulsed. The outputs are made to pulse by a pulse command in the PROM controller. The trip and data outputs can be loaded into any of the storage registers.

REGISTERS

There are eight numerical registers used to store intermediate values in the ASIC, and there are eight single-bit registers used to store the trip outputs. Storing a number in a register is done in one clock cycle.

ADC INTERFACE

There can be up to eight ADCs interfaced to the ASIC. The ADC interface controls these ADCs, reads the data from them, and makes the data available for storage in registers A through H. The inputs from the ADCs can be either serial or parallel, and the ADCs can have 12-, 14-, or 16-bit outputs. The PROM controller selects an ADC for conversion. The ADCs are bipolar.

DAC INTERFACE

There are two DACs that interface to the ASIC either through the 17-bit DAC bus or through the system data bus.

ASIC COUNTER

The ASIC counter steps the controller PROM. The function selection header on the Personality Module selects the beginning location in the PROM, and the ASIC counter increments the PROM from that location. The counter counts to a preset maximum and then resets to zero.

2.7.3 ASIC Design Features

All of the math-based circuits, ADC/DAC interfaces, registers and counter/controller circuits have been designed and implemented in the ASIC.

Features of the ASIC design approach are summarized below.

- Computations are done sequentially to avoid timing problems.
- The clock runs significantly slower than the circuit capability. This feature avoids timing problems such as race conditions and eliminates the effects of parasitic capacitance.
- Circuits are designed by combining and testing modules at each level from bottom to top.
- Standard cells and custom designed (bit-sliced) cells are used to make circuit primitives.
- Primitives are combined to make basic functions.
- Basic math functions are combined to implement the process function.
- Process functions can be completely verified and tested.
- There are no undefined states or conditions that can "hang" the system.

- Tests are performed at each design stage, and tests of the basic functions are repeated on the fabricated ASIC.

2.8 CONTROLLER

Refer to Figure 2-3. The Controller is a 64K Programmable Read Only Memory (PROM) that is divided into "segments". A segment is defined as a block of memory locations in the Controller that contain the control codes that actuate the math circuits in the ASIC. Each math circuit and function in the ASIC has a unique control code that controls its operation. As the segment sequences through the control codes, the math circuits in the ASIC are enabled (one at a time) in the proper order to perform a process function. For example, to implement a lead/lag process function digitally, the Z-Transform is used and consists of 3 multiplications and 2 additions. The lead/lag segment in the Controller will enable the ASIC multiplier circuit three times and the adder circuit two times.

A separate Controller segment was designed for each style of 7300 card to be replaced. The Personality Module (refer to Section 2.9) is used to select the proper segment to replace a given 7300 card. Thus, when the Lead/Lag Personality Module is inserted into the Main Board, the lead/lag segment in the Controller will be selected and the ASIC will perform the required math functions in the proper sequence

The control codes within a Controller segment are sequenced (or stepped) by a counter in the ASIC. When the counter reaches 1024, the counter starts over, thus repeating the process function. Since the clock runs at 1 MHz, the cycle time for any one segment is 1.024 ms. The basis for this design approach is to have a fixed cycle time. This approach facilitates the implementation of time dependent functions such as lead/lag. The cycle time of the segment running on the ASIC chip is small compared to the response time of the 10 Hz input filter. Typical time response budget for the analog cards/modules in a process protection channel is approximately 150 ms. Overall protection channel system time response (from process variable step change to rod drop) typically ranges from 1-6 seconds. Failure of the counter is detected by the General Alarm circuit (refer to Section 2.10).

A control code is an 8 bit binary word that enables a math circuit or function in the ASIC. For example, control code 00000101 enables the divider circuit in the ASIC. When this control code is issued by the Controller to the ASIC during one of the segments, the ASIC will perform the divide operation. With 8 bits, a total of 256 unique control codes can be defined.

Compliance with the design constraint prohibiting any software or programmable code in the design (refer to Section 2.0, Item 4) is demonstrated by the following features.

(1) Each control code controls a specific math circuit or function in the ASIC. The control codes are unique and independent of each other. The control code being issued was not determined by the previous control code, nor does it have any bearing on the control code that follows.

(2) There are no decisions being made on the input data or as the result of a mathematical function. When a control code is issued, the ASIC circuit or function is performed regardless of the value of the inputs or data.

(3) Since there are no decisions being made on the data, there is no branching or alternate signal paths. The ASIC performs its operations in accordance with the sequence of control codes being issued by the controller.

(4) The system cannot "halt", "hang" or "lock-up". As long as the clock circuit is running, the ASIC counter is counting, the Controller is issuing control codes, and the ASIC is performing the functions defined by the control codes. Failure of the clock circuit is detectable and will result in an alarm (refer to Section 2.10).

(5) Operation is deterministic and sequential, with no interrupts. The control codes will be issued according to the pre-determined sequence which cannot be altered or interrupted. When the end of a segment is reached, the sequence starts over. Upon momentary power interruption, the counter and segment will restart automatically without manual intervention.

(6) If during a sequence a control code becomes corrupted (missing a bit or a bit changes), the ASIC will perform the function defined by the "new" control code. This will produce an incorrect result. If the failure is momentary, the correct function will be performed by the ASIC during the next cycle. If the failure is permanent, the output will not be correct and therefore will be detected during periodic channel operational testing or via direct observation (e.g., incorrect indication).

(7) The control codes enable dedicated circuits in the ASIC. As stated earlier, each circuit is dedicated to performing only the function for which it was designed. The circuits are either ON or OFF and are not programmable.

(8) Operation of the ASIC does not rely on critical timing relationships.

(9) A process function (i.e., lead/lag) is performed by arranging the control codes within a segment in such a manner that the ASIC math circuits or functions are enabled in the proper sequence. If an incorrect control code appears in the sequence, the desired process function will not be obtained. If the failure is permanent, the output will not be correct and therefore will be detected during periodic channel operational testing or via direct observation (e.g., incorrect indication).

(10) For undefined mathematical operations, such as divide by zero, the ASIC will set an error flag (as stated in Section 2.7) and continue operation.

(11) Correct operation of the ASIC math circuits can be verified during the fabrication process as part of the post-seal testing. This provides assurance that the ASIC

component does not contain any latent failures or flaws that would inhibit proper operation.

(12) Correct operation of the process function (i.e., lead/lag) can be verified after the card/module has been configured.

2.9 PERSONALITY MODULE

The Personality Module (PM) is a plug-in module that is used to configure, or "personalize", the Main Board to perform the desired process function to be implemented. There will be a PM that corresponds to each 7300 System card style included in the scope of the program (refer to Section 2.1). The PM performs three functions to "personalize" the Main Board. The first is to select the starting address of the segment in the Controller that contains the desired process function. The second function is to provide additional components that modify the input and/or output signal conditioning circuits. The third function is to align the input and output signals to the proper pin assignments on the 42-pin card edge connector.

When the PM is inserted onto the Main Board, the desired process function will be selected automatically. This is accomplished by grounding certain pins on the Controller via the PM. This identifies the starting address for the desired process function segment. As stated in Section 2.8, the counter inside the ASIC chip steps the Controller until all 1024 steps have been executed. Upon completion, the segment (and process function) repeats.

The PM contains electronic components that are unique to a given card style. Placing these components on the PM is more cost effective than locating them on the Main Board. This contributes toward reducing the cost of the Main Board because the components on the PM are unique to a given 7300 card style and will not be part of every Main Board. As an example, the 7300 System Summing Amplifier Median Signal Selector (NSA Group 5) contains a relay that selects one of the three inputs as the default output in the event of loss of power to the card. This relay is located on the PM for the MSS application rather than placing the relay on the Main Board. Other components located on the PM are resistors for input summing junctions, capacitors, diodes, power supplies, and operational amplifiers that provide additional input signal conditioning.

The PM aligns the inputs and outputs of the Main Board to the proper card edge pin assignments. In the 7300 Series hardware, all signals enter and exit the card via the standard 42 pin card edge connector. The Main Board design approach described herein has approximately 100 input and output points. Only the I/O points necessary to implement a given process function are required, and they must be connected to the same card edge point that was assigned to the analog module.

When the Personality Module is inserted onto the Main Board, the desired process function will be selected, additional components will be added to replicate the analog module, and the I/O

pin alignment will be accomplished. The design approach has the following advantages.

- The process function selection is passive (i.e. accomplished by grounding of controller pins to identify the process function segment).
- The PM makes the Main Board pin-for-pin compatible with the 7300 card style it replaces.
- The process function selection and pin alignment are coordinated to prevent configuration errors.
- Locating unique components on the PM contributes to reducing the overall cost of the Main Board.

2.10 INDICATORS, ALARMS AND TEST POINTS

Refer to Figures 2-2 and 2-4. Indicators, alarms and test points have been incorporated into the design to comply with the design constraints to minimize impact on existing plant procedures, maintenance and test equipment (refer to Section 2.0, Items 10 and 11). The design approach has been to keep the design simple with little or no diagnostic features.

INDICATORS

There are 2 LED indicators on the front edge of the Main Board; a red LED for the General Alarm and an amber LED for the Trouble Alarm.

GENERAL ALARM INDICATOR

A red LED is used to indicate the status of the General Alarm function. The General Alarm function replaces the "Power Supply Failure" alarm normally located on Pin 3 of the 7300 Series cards. Since the General Alarm is indicated in the Main Control Room, the design approach to minimize "nuisance alarms" is to alarm only permanent failures such as failure of the ASIC circuits or card power supply circuits (regulators, fuses, etc.). Transient conditions, such as the ASIC errors described in Section 2.7 (i.e., dividing by zero leading to a temporary overflow condition) are not alarmed. The General Alarm circuit is located on the Main Board, and it monitors the on-board power supplies, the RAMLogic FPGA, and the ASIC monitor pulse. The output of the General Alarm circuit is normally energized, which applies an open circuit to Pin 3 and illuminates the red LED, indicating that the card is energized and operating normally. Upon failure of any of the on-board power supplies, or failure of the RAMLogic FPGA to configure, or failure of the ASIC monitor pulse, the output of the General Alarm circuit will apply a ground to pin 3 of the card edge connector. This will activate an alarm in the Main Control Room (if so-wired in the plant). This will also extinguish the red LED on the front edge of the card. In Median Signal Selector applications (NSA Group 5), the General Alarm circuit will also de-energize the relay on the NSA Personality Module which will switch the pre-selected analog input as the default output.

The ASIC Monitor Pulse (AMP) is generated by the ASIC chip every cycle at the end of the segment and is connected to a deadman timer circuit. The output of the deadman timer circuit is normally energized as long as the AMP occurs every cycle. The AMP will stop if any of the following occur:

(1) The 1 MHz clock circuit fails;

(2) The Controller fails (i.e., the ASIC stops getting control codes);

(3) The address generator in the ASIC fails; or

(4) The ASIC itself fails.

TROUBLE ALARM INDICATOR

An amber LED is used to indicate the status of the Trouble Alarm function. The Trouble Alarm circuit is part of the RAMLogic FPGA located on the Main Board. It monitors the Operator Interface circuit, digital output overcurrent conditions, and the ADC self-calibration. The output of the Trouble Alarm circuit is normally de-energized, and the amber LED is off. Upon failure of the Operator Interface circuit to properly configure when energized (refer to Section 2.6), or an overcurrent condition detected on the NAL PM output, or failure of the ADCs to self-calibrate, the output of the Trouble Alarm circuit will energize. This illuminates the amber LED on the front edge of the card. The Trouble Alarm signal does not leave the card.

NAC AND NAL INDICATORS

Red LED's are located on the front edge of the NAC and NAL PMs to indicate the on/off state of the current sinking transistors in the low-side switch circuitry of the digital actuation outputs. The transistors in this circuit can be either normally energized (NE) or normally de-energized (ND). These LED's replicate the indicators found on the 7300 Series NAL and NAC cards.

TEST POINTS

There are approximately 27 test points on the Main Board. Seven test points are located on the front edge of the card to measure output signals. The other test points are located throughout the card to facilitate measuring power supply voltages and intermediate signals. Test points are also located on the front edge of Personality Modules where necessary.

2.11 TESTING

Testing can be categorized into four areas: (1) component testing, (2) qualification testing, (3) production/factory testing, and (4) site testing.

COMPONENT TESTING

The main components are the ASIC chip and Controller. Every ASIC chip is tested at the component level as part of the fabrication process. During post-seal testing, the ASIC chip undergoes a MIL-STD-883 burn-in test. This test is conducted at 125 Degrees Celsius for 160 hours and is intended to reduce failures attributable to infant mortality. After burn-in testing, the ASIC chip undergoes a suite of tests designed to verify proper operation of the math circuits and functions inside the ASIC. These tests are done on all of the fabricated ASICs to confirm that the fabrication process was correct. The ASIC Monitor Bus is used during these tests. The ASIC Monitor Bus is connected to internal points inside the ASIC that are not accessible at the ASIC pins. It was designed into the ASIC for use during design and fabrication testing to comply with the design constraint for the ASIC to be completely testable at the component level (refer to Section 2.0, Item 5). The purpose of the Monitor Bus is to reduce the number of test vectors required for extensive ASIC testing. The Monitor Bus is eight bits wide and is enabled by a Monitor Bus control line. During factory acceptance testing, the Monitor Bus is connected to an automated testing machine that compares measured values to expected values to confirm that the ASIC is functioning properly and that there are no latent failures (such as shorts, opens, a transistor stuck at one or zero, or two outputs shorted together) in the ASIC math circuits or functions. A certificate of conformance (C of C) accompanies each production run of ASICs.

The Controller contains the control codes that enable the ASIC math circuits and functions (refer to Section 2.8). The Controller PROM is tested by check-sum verification after all of the segments have been configured.

QUALIFICATION TESTING

Qualification tests are one-time type tests performed to qualify the component or system for Class 1E applications. The ASIC-based replacement modules are tested to validate that all process functions perform as intended. For the card styles used in protection systems, these tests are performed under the extremes of temperature, humidity, seismic and EMI/RFI environs. Cards that are used as isolators (NLP and NSC) are tested for fault withstand capability. In addition, Abnormal Conditions and Events (ACEs) tests are performed. These tests check over-range and recovery, variations in power supply voltage and frequency, operator error, etc.

Upon successful completion of qualification testing, the ASIC and Main Board/Personality designs are qualified for Class 1E applications. For the ASIC chip, maintaining the Class 1E qualification and compliance to 10 CFR Part 21 is achieved by repeating the post-seal test. For the Main Board and Personality Modules, maintaining the Class 1E qualification is via design and configuration management control.

PRODUCTION/FACTORY TESTING

Each ASIC-based card assembly under-goes alignment, calibration and testing at the factory. Factory alignment and calibration consists of adjusting the DAC gain and offset potentiometers

in the analog output and Operator Interface circuits. Each Main Board assembly and Personality Module under-goes a functional test to verify proper operation.

SITE TESTING

The design approach maintains the existing method of conducting periodic surveillance testing (i.e., channel calibration and operational testing). The 7300 System channel test cards (NCT, NTC and NMT) are not included in the scope of the design effort. Verification of proper operation of the ASIC-based module does not require special test provisions, which complies with the design constraint to minimize the impact on existing plant procedures (refer to Section 2.0, Item 10). A small degree of revision to existing site test procedures is envisioned because calibration and/or scaling for test points (if required) and entering/changing setpoints and tuning constants for the ASIC-based replacement module is different than the analog counterpart.

The ASIC Subgroup indicated that existing site test procedures will be revised to direct I&C personnel to the ASIC Instruction Manuals for card operation. In addition, where appropriate, test point specific scaling values will also be included in the calibration procedures. When an ASIC-based replacement module is installed in a cabinet and the setpoints and tuning constants entered via the Operator Interface, verification of proper operation will be accomplished by performing a channel operational test/calibration verification using approved plant procedures.

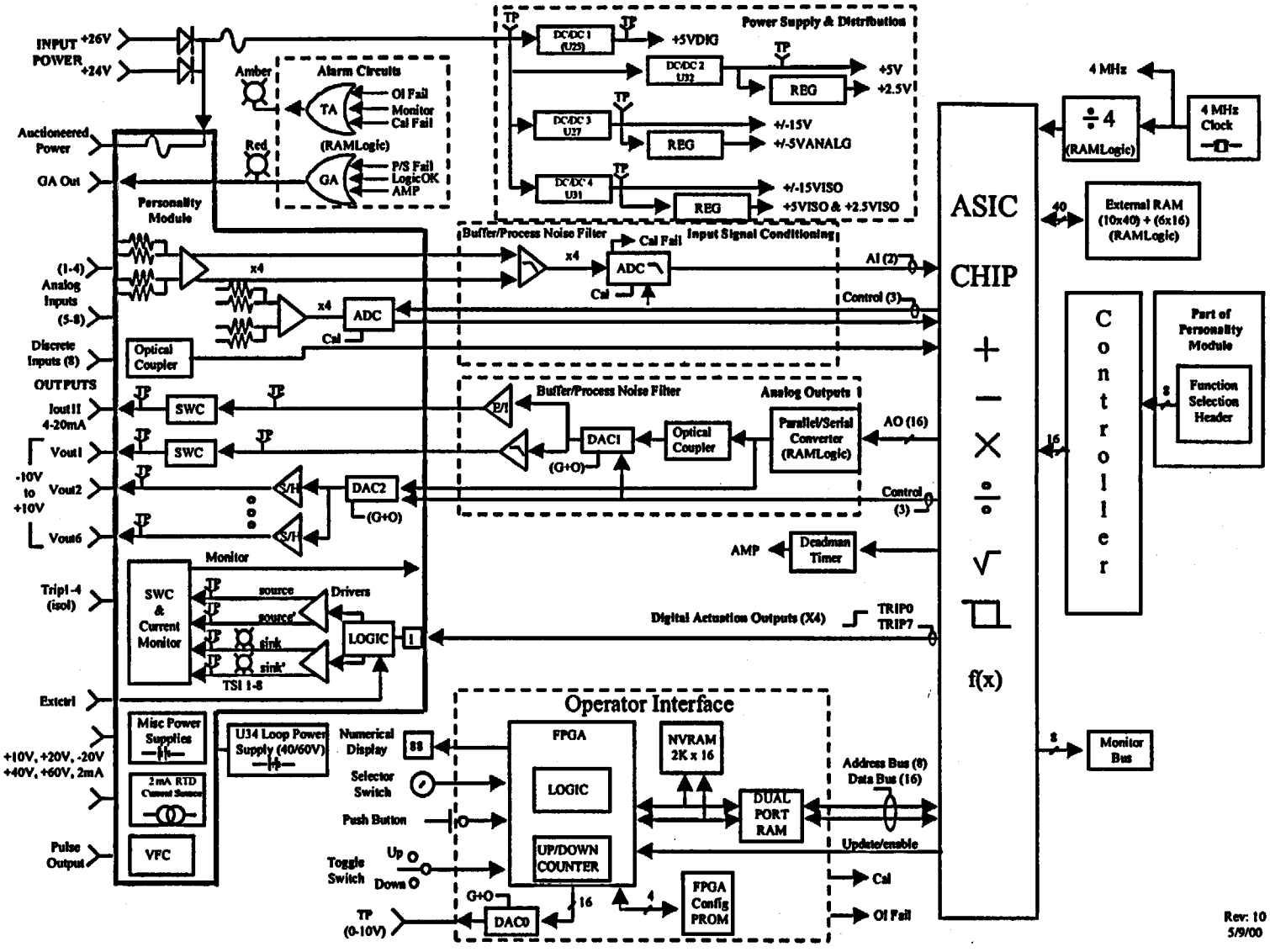


FIGURE 2-1 ABRM BLOCK DIAGRAM

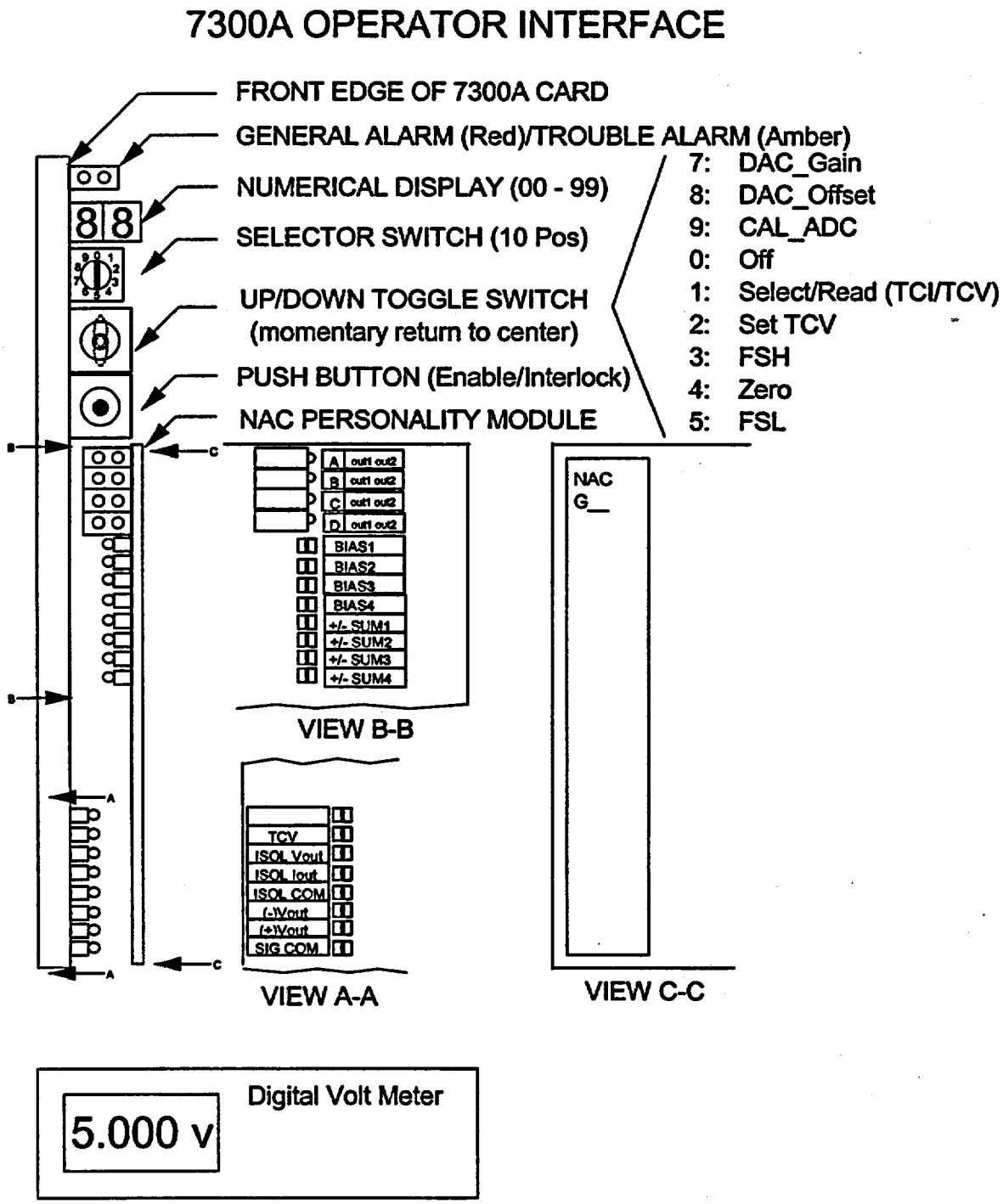


FIGURE 2-2 ABRM OPERATOR INTERFACE

SEGMENT	NAME
01	NAC Comparator (GO1)
02	NAL Comparator (GO1-3)
03	NCB Controller (P)
04	NCB Controller (PI,PID)
05	NCB Controller (FFI)
06	NCB Controller (FFII)
07	NCD Driver (GO1-4)
08	NCH Function Gen. (GO1-13)
09	NLL Lead/Lag
10	NLL Lag
11	NLL Rate Lag
12	NLP Loop P/S (GO1,2,4)
13	NLP Isolator (GO3,5)
14	NMA Mixing Amp (GO1)
15	NMD Multiplier/Divider
16	NMD Square Root
17	NRA RTD (GO1,3) NR, Linear
18	NRA RTD (GO2,4) WR, Linear
19	NRA RTD (GO1,3) NR, Exact
20	NSA Summing Amp (GO1,2)
21	NSA Summing Amp (GO3)
22	NSA Summing Amp (GO4)
23	NSA Summing Amp Hi Med Select
24	NSC Signal Conv (GO1-8)
25	NTD Track Driver (GO1,2)
26	NVP V/P Conv (GO1,3)
27	NVP V/P Conv (GO1,3)
28	NVP V/P Conv (GO2)
29	NSA Summing Amp (GO5)

FIGURE 2-3 ABRM CONTROLLER

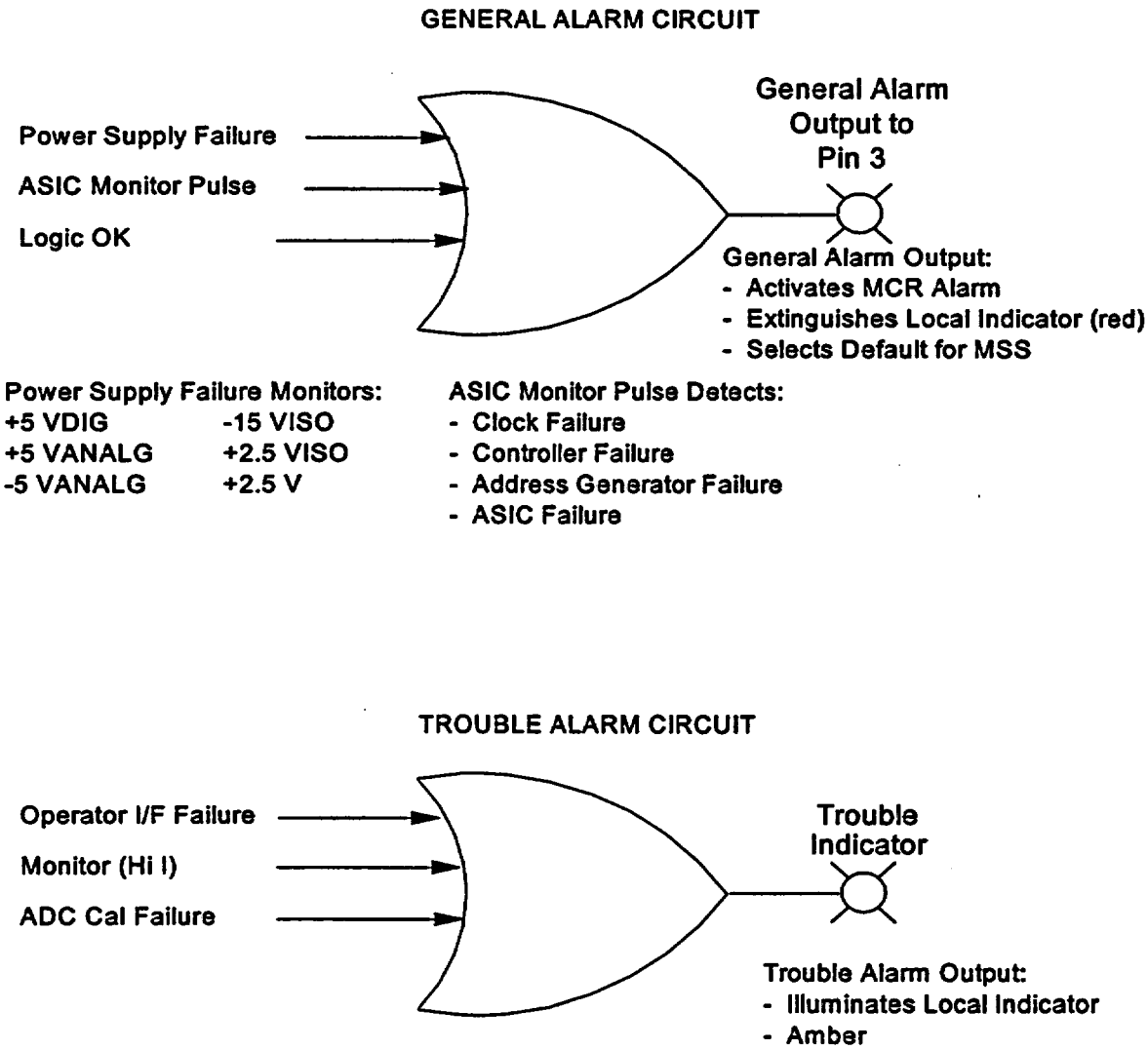


FIGURE 2-4 ABRM ALARM CIRCUIT LOGIC

3.0 DESIGN VERIFICATION AND VALIDATION PROCESS

The ASIC-Based Replacement Module development program Design, Verification, and Validation Plan, Reference 3.3.1, was developed to assure that a disciplined process was followed in the development of ASIC-based replacement cards, given multiple organization involvement in the program. Organizational procedures have been followed but in some cases need to be supplemented by specific program plans.

3.1 DESIGN PROCESS

Several different design organizations participated in the ASIC-Based Replacement Module development program. Westinghouse Electric Company (WEC) was the program technical lead responsible for the primary design, verification, validation and licensing activities. As a 10 CFR 50 Appendix B supplier, WEC has procedures in place to perform design, verification, and validation activities for basic components produced, as well as for commercial grade components supplied by others. For design activities performed outside WEC, WEC performed independent review of the design and conducted tests during validation testing to confirm adherence to requirements.

WEC was responsible for assuring that design, verification and validation activities were performed in a manner which maintained the review process independent from the design process. Within this context, independence means an objective second-party review by competent individual(s) of material that they did not design. This was accomplished by performing an internal second-party review of all design documentation, or by auditing vendors to assure adherence to the design and review process. Second-party review of design documentation was indicated by sign-off.

Westinghouse was responsible for the following program activities:

1. Project definition
2. Conceptual design
3. Project specific methods and activities
4. Functional requirement definition (process functions, algorithms, etc.)
5. Hardware requirement definition
6. Analysis
7. Technical integration of all design areas (Main Board, Personality Modules, ASIC, Controller)
8. Main Board design, layout and assembly
9. Operator Interface design
10. Personality Module design, layout and assembly
11. Configuration Management Control

12. Documentation (specifications, design drawings, manufacturing drawings, etc.)
13. Second party review of all ORNL design activities (e.g., Controller algorithm verification)
14. Reliability Assessment and Failure Modes and Effects Analysis
15. Design Reviews (Preliminary, Intermediate and Final)
16. Validation Testing of integrated product
17. Abnormal Conditions and Events Testing (ACEs)
18. Qualification Testing of integrated product
19. Licensing, including regulatory compliance analysis
20. Prototype and production unit fabrication
21. Commercial Dedication of ASIC
22. Technical Manual

Oak Ridge National Lab (ORNL) was responsible for the design of the ASIC chip and Controller. ORNL was not an Appendix B supplier and was treated as a commercial supplier in the plan.

ORNL was responsible for the following program activities:

1. ASIC design and layout
2. ASIC prototype fabrication
3. Controller design
4. Controller code development

Northrop Grumman Advanced Technology Center (ATC) was responsible for conducting simulation testing of the ASIC chip design, fabrication of ASIC chips, and for performing comprehensive testing of the chip prior to release to Westinghouse. Northrop Grumman was not an Appendix B supplier but works under strict mil-spec procedures.

Northrop Grumman ATC was responsible for the following program activities:

1. Simulation testing of ORNL ASIC design
2. ASIC prototype testing
3. ASIC fabrication for qualification and production
4. ASIC component testing

3.2 VERIFICATION PROCESS

The overall objective of the design verification process was to independently confirm, by means other than accomplished by the designer, that the final design functions as documented. Design verification was accomplished by conducting formal design reviews and performing simulation testing to determine the performance of the design as a separate entity, without the use of actual system hardware.

The design verification process divided the overall system design into smaller "subsystems" for evaluation (for example, an analog input circuit or a digital output circuit). After all "subsystems" were verified, the complete system was evaluated. This design verification philosophy ensured that all subsystems and interfaces between subsystems were reviewed and/or tested. The techniques used in the design verification process fell into two basic categories: design reviews and simulation testing.

3.2.1 Design Reviews

Design reviews were performed by individuals independent from those who designed the system. The technical qualifications of the individuals participating in the design reviews were comparable to those of the designers. There were three types of design reviews conducted during various phases of the development process: Preliminary Design Review, Intermediate Design Review, and Final Design Review.

The Preliminary Design Review was performed by representatives from utilities that were members of the ABRM Steering Committee. These representatives were familiar with the operation and application of the analog modules. This approach provided assurance that the replacement module would perform as intended.

The Intermediate Design Review was performed by an independent designer. The Main Board and Personality Module designs were reviewed against the specification requirements.

The Final Design Review was performed by a combination of independent designers, training instructors, manufacturing personnel and utility representatives.

Results of the design reviews were documented in written reports.

3.2.2 Simulation Testing

During the Implementation Phase of the development program, component selection and drawings documenting the design were completed. At this point, simulation testing of the design was performed to verify that the functionality of the design meets the applicable design specifications. Simulation testing is a design verification method that attempts to comprehensively exercise (via computer emulation) the design of a system, subsystem or component. In effect, the operation of the system is simulated to confirm that it agrees with the specifications. The functionality of the design was verified along with any supporting "subsystems" necessary to implement the required function.

Simulation testing was used to verify the transformation from a "paper design" to actual hardware. The actual hardware was modeled for observation and understanding, making full verification at this level feasible.

Simulation testing required that the design be understood before selecting the test inputs, commonly called "test vectors". The test inputs (or test vectors) were developed to exercise all possible signal paths through a system or component, and operation was compared to expected results. Where this was not possible, the test inputs were chosen to exercise as many components as possible. For components or system operation not directly observable, a qualitative analysis was performed to assess the significance of the components not exercised.

Simulation testing can be used to evaluate the system response to potential unintended functions (i.e., transients, noise, etc.). The simulation process can also be used to evaluate interactions between subsystems (i.e., loading, opens, shorts, etc.) and to ascertain postulated failure modes and effects.

After the simulation testing verified that all requirements were satisfied, the design was released for fabrication and subsequent system validation testing.

3.2.3 Controller Verification

Design, verification and validation of the ASIC Controller warranted special consideration because of the similarity to "software". Due to the simplicity of the design approach and "hard-wired" concept of the ASIC chip, the Controller design can be thoroughly tested. Because this program was for a replacement module for an analog system, the process functions were defined in the instruction bulletins for the analog hardware. The instruction bulletins, in conjunction with the Main Board design specification, provided the functional requirement input to the Controller design. The Controller design specification decomposed the functional requirements into algorithms (e.g., a lead/lag function). Each algorithm defined a sequence of math operations (e.g., add, subtract, etc.) to be performed by the ASIC. The Controller code was verified to the extent that the code reflects the intended operation (add, subtract, etc.). The sequence of operations implemented via the Controller code was validated during formal validation testing of the integrated product. For example, the Controller code that implements a lead/lag function was tested during validation testing. Validation testing demonstrated that all Controller algorithms performed the intended process functions, and performed in a known and predictable manner when subjected to abnormal conditions and events.

The Validation Process is discussed in Section 5 of this report.

The ABRM Design, Verification and Validation Plan, 413A62 was submitted to the NRC via Reference 3.3.2.

3.3 References

3.3.1 Westinghouse Specification 413A62, Revision 0, ABRM Design, Verification and Validation Plan.

3.3.2 WOG Letter OG-97-069, dated 7/10/97, Initial Submittal of Application Specific Integrated Circuit (ASIC) Design Information.

4.0 ASIC CHIP TEST RESULTS

4.1 INTRODUCTION

The ASIC is a custom integrated circuit that is designed to implement process monitor and control functions in the protection and control instrumentation systems of nuclear power plants. The ASIC is a new concept in protection and control instrumentation design because it applies digital processing technology to implement analog circuit functions, and it does so without the need for complex computational circuits, such as microprocessors and computers. In operation it will perform many of the functions of an embedded processor, but it is entirely deterministic and will therefore not be susceptible to system crashes, latch-up or other problems often encountered with programmed processor circuits.

The ASIC was designed to avoid some of the problems associated with a software-based system. Significant advantages of the ASIC design are that only the required functions are included in the device, and these functions are "hardwired". Because the functions are hardwired and because the ASIC is designed to have access to the inputs and outputs of these functions, test vectors can be developed to detect component failures. The ASIC circuits and their control components are designed such that there are no undefined states where the system can "hang". If there are no component hardware failures, each ASIC-based module implements its safety algorithm continuously. There are no interrupts, loops or branches that make decisions based on measured data, or undefined states. Each step is defined and repeated continuously in a loop. The ASIC design is structured to avoid these problems which may occur in software and are also difficult to find by testing.

The ABRM Project Design, Verification and Validation Plan identified the responsibilities of the various participating organizations. The ASIC chip design, verification and validation were performed in accordance with the design process outlined in Section 6.1 of the plan. Westinghouse was responsible for functional requirement definition, hardware requirement definition, integration testing and validation testing. Oak Ridge National Laboratory (ORNL) was responsible for the ASIC design and layout and for fabrication of prototype chips for evaluation. Northrop Grumman Advanced Technology Center (ATC) was responsible for simulation testing of the ORNL ASIC design, testing the ASIC prototypes, and fabrication and testing of ASIC chips for qualification and production. This process provided assurance that design, verification and validation activities were performed in a manner that maintained the review process independent from the design process. Within this context, independence means an objective second-party review by competent individual(s) of material that they did not design. Reference 4.8.1 submitted the plan to the NRC to facilitate ongoing review and acceptance for referencing in licensing actions.

4.2 ASIC CHIP DESIGN PROCESS

The ASIC chip design requirements are identified in References 4.8.2, 4.8.3, 4.8.4, and 4.8.5. The chip design specifications were written based upon the requirements to replace safety system analog cards currently used in nuclear power plants, i.e., the ASIC-based modules are to be

equivalent replacements for the 7300 System analog cards. These specifications were used to develop the basic functional modules for the ASIC chip.

The ASIC chip design was simplified by structuring the ASIC to consist of simple modular circuits that can be designed and tested independently of each other. The ASIC architecture contains hardwired circuits organized into functional modules that are physically separated from each other. The functional modules can be accessed from the input and output pins of the ASIC package. Each of the functional modules is built hierarchically to simplify design, testing and operation of the ASIC. The ASIC chip contains one each of the following functional modules:

- Multifunctional Adder (MFA) (adder, subtractor, two's complement, shift left and right, and absolute value functions);
- Multiplier/Divider;
- Square Root;
- Comparator;
- Analog-to-Digital-Converter Interface (ADC);
- Digital-to-Analog Converter Interface (DAC);
- Storage Registers; and
- Counter.

At the very top of the hierarchical design is the ASIC with its inputs and outputs. The next level has the eight basic functional modules identified above and all interconnections between them. At the next level are the logic blocks that comprise the functional modules. A logic block consists of logic gates (e.g., NAND, NOR, etc.) arranged such that they perform a function, such as a 2-bit adder. Eventually, at the bottom of the hierarchy, are the primitive cells (transistors) used to implement the hardwired logic gates. Figure 4-1 depicts a standard primitive cell for a 2 input NOR gate. A functional module may contain 40 of these gates if a 40 bit NOR function is required. This approach was used throughout the design of the ASIC chip as well as the development of the test vectors.

To design the ASIC, ORNL used primitive cells obtained from industry standard libraries to construct a logic block (such as a 2-bit adder) and tested it to confirm that it performed as required. After the logic blocks were designed and tested, they were assembled into functional modules (a 40-bit adder), which were then tested with a command file, and revised if necessary. The functional modules were then assembled into the ASIC core and tested again. The final design consists of eight basic functional modules that were designed and tested at each stage, from the bottom up. Figure 4-2 depicts the functional block diagram of the ASIC chip.

The core layout was done after the ASIC core design was completed as described in the previous paragraph. The layout, which was still part of the design phase, was tested using a timing-based simulator. Because the ASIC application is much slower than its tested capability, timing is not a problem. If problems or improvements are identified during the timing simulations, the design can be revised and re-tested. After the core design and layout were completed, the input and output pads were added and the design was tested again with the timing-based simulator. The functional tests used for logical and timing performance were selected to test the design for normal and for extreme (or boundary) conditions.

The ASIC chip design consists of a set of electronic files that describe how the primitive cells are hardwired together to form the functional modules. The electronic files are converted to silicon by the foundry (ATC). Before release to ATC, ORNL performed functional tests on the design simulation. The design simulation is a model of the design that contains all of the primitive cells. Each of the eight functional modules was tested with a set of functional and fault test vectors. The test results are documented in References 4.8.14 and 4.8.15. When these tests were completed, the design was submitted to a foundry for fabrication.

In compliance with the Design, Verification and Validation Plan, ATC repeated the design simulation testing using the same test vectors used by ORNL. ORNL sent Northrop Grumman the Viewlogic schematic, library and functional simulation input and output files for the ASIC in their native Viewlogic formats. Simulations were repeated at Northrop Grumman and results were compared with ORNL simulation result files to assure that the data was transferred properly and the tools were acting consistently. Since the functional test patterns were relatively short, they were concatenated into a single file. An initialization sequence was added to the simulation pattern to guarantee that the ASIC state is synchronized with the state predicted by the simulator before the actual test sequence is started. The simulation was then run and the input and output states vectorized (sampled at regular intervals) so that the results were compatible with ASIC testers.

After analyzing the utility of the functional test vectors in detecting manufacturing flaws, Northrop Grumman consulted with ORNL on creating a set of fault vectors to supplement the functional vectors. Timing as well as stuck-at fault issues were addressed. The same transfer process was applied to the fault simulations as the functional simulations.

The address counter circuit required a special test configuration and vectors, since the tester must be synchronized to the part. This test exhaustively exercises the address counter circuitry and its outputs. The address counter circuit test is performed at package level test only. ATC test results are documented in Reference 4.8.19.

After fabrication, the ASIC chip was functionally tested to confirm that the design was correct, and tested with enhanced fault test vectors to detect failed components within the chip. The enhanced fault test vectors applied to the fabricated ASIC were developed with the intention of operating every gate in the chip. It is not feasible to test every combination of inputs, but it is feasible to test all gates within the ASIC. Although it is possible to develop test vectors that operate all gates in an ASIC, there may be problems observing operation of these gates because they cannot be accessed from the output pins. To resolve this, the number of gates that can be

observed during factory acceptance testing was greatly increased by including the Monitor Bus in the ASIC design. The Monitor Bus is an eight-bit wide data bus connected to the internal circuits not accessible at the chip boundary. It is only used during factory acceptance testing and is not accessible when the ASIC chip is mounted on the Main Board. The Monitor Bus is made to run at a higher speed than the clock controlling the other functional modules in the ASIC so that it can observe transitions of the internal circuits. It monitors asynchronous circuits, and it monitors internal circuits that operate in more than one clock cycle. This Monitor Bus added circuitry and some complexity, but it increased the degree of fault coverage of the test vectors. Fault coverage is the ratio of the number of gates tested to the total number of gates in the ASIC. Per Reference 4.8.18, the combination of functional and fault test vectors result in 99.8% fault coverage. Figure 4-2 shows the Monitor Bus connection to the functional modules.

4.3 DESIGN VERIFICATION PROCESS

Because of the critical application of the ASIC in a protection system, the ASIC must be either free of design and processing issues, or its behavior must be entirely characterized so that all issues in design or production are known and can thus be accounted for in its application circuits. Such characterization can only come through extensive testing of both the design and fabrication of the ASIC.

The testing program for the ASIC originally started before the chip was fabricated. Test vectors were used extensively in the verification of the design to provide reasonable confidence that the chip would work as designed. The original tests were created by the chip designers (ORNL) and consisted of over 200,000 test vectors to determine if the chip was performing as designed.

Verification can be accomplished by two types of tests. The first type, which is design testing, confirms that the chip's circuits are operating as they are designed to operate. This type of testing performs detailed tests on the chip to confirm that each gate, or other low-level circuit element, is performing the job that it was designed to perform. Design verification confirms that the chip's circuits are working properly, but it cannot confirm that the circuits were designed properly to begin with. The second type of test, which is functional testing, will determine if the design is properly implementing the desired circuit functions, but it will not determine if all the circuits are working properly. A complete testing program requires that both types of tests are used to confirm that both the design and the circuits that implement it are all working properly. If the testing program neglects the functional test, the chip's circuits will be verified to be working as they are designed, but they won't be verified to be implementing the correct function. If the design test is omitted, the chip's circuits will be verified to be implementing the desired functions, but they won't be verified to be entirely operational.

4.3.1 Original Test Program

The original testing program for the ASIC implemented a detailed and thorough design test of the chip. Each circuit in the chip was tested in great detail and was shown to be working exactly as designed (References 4.8.14 and 4.8.15). However, this testing program, due to a number of factors, did not include a sufficient functional test. Because of this, the chip was

tested thoroughly for operational compliance with the design of the circuits, but the design itself was not tested for compliance with the functional specifications. Thus, even though the tests confirmed that the circuits were working properly, they did not reveal design flaws in the circuits themselves.

The testing oversight that failed to perform a thorough functional test of the chip allowed a design flaw to go undetected until it appeared as an unexplained error in the computational result of the chip's Multiplier/Divider functional module (Reference 4.8.16). The error was discovered during Westinghouse integration testing of the chip mounted on the Main Board. It was during the investigation of the design flaw that the deficiency in the functional test was discovered. In order to completely verify and characterize the chip's operation, and alleviate further doubts about the design of the chip, a new functional testing and vector verification program was commissioned at ORNL.

4.3.2 Revised Test Program

The new testing program was intended to perform a more detailed and extensive series of functional tests that would completely characterize the ASIC and verify the functional design of the chip in addition to the design verification that was conducted in the first test. It was also intended to fulfill the testing goals that were not fully realized in the first test due to insufficient thorough functional tests.

The first step in the new testing process was to codify and organize the functional requirements of the ASIC. These requirements were already in textual form in three documents: the ASIC Design Specification, Reference 4.8.3, which detailed physical specifications such as I/O pin characteristics along with a brief overview of the functional requirements of the design; the ASIC Functional Description Reference 4.8.5, which described the various chip functions and how they would work; and the ASIC Interface Specification, Reference 4.8.4, which provided detailed information on the operation of the chip and how it should interface to external components.

Each of these three documents was decomposed so that the textual information was broken down into a series of brief statements, each of which would describe a single requirement. In this way the testing program could address each of the requirements separately, thus ensuring that every operational and functional requirement of the chip was tested.

4.3.3 Functional Requirements Decomposition

Westinghouse decomposed the ASIC requirements contained in the ABRM Main Board and Personality Module Design Specification. Four engineers at ORNL conducted the decomposition of the three ASIC specification documents. The engineers divided the documents among themselves and independently decomposed their part of the requirements. Collectively the result of this effort was a complete ASIC functional decomposition matrix, Reference 4.8.6, in which every requirement was listed in a separate statement.

Eight functional requirement documents were created from this stage. Because there was significant overlap in the original specification documents, the resulting functional requirement decompositions also included topic overlaps. When combined, the documents generated 763 individual requirements for the ASIC (Reference 4.8.17).

4.3.4 Testing Criteria

The next step in the testing process was to define test criteria for each of the decomposed requirements from the previous step. The criteria, when implemented in test vectors, were intended to exercise the ASIC in a way that would confirm that it fulfills each particular functional requirement. The number and complexity of the test criteria varied between requirements, and in many cases a single series of test criteria could be used to test more than one requirement at a time.

The eight original functional requirement files resulted in fifteen test criteria files. The test criteria files, with their contents and the functional requirement files from which they were derived, are listed in Reference 4.8.17. The information provided includes the file names containing the test criteria, the file containing the functional requirements used to develop the test criteria, comments on the types of tests and on the functions being tested.

4.3.5 Test Vectors

The criteria files, which are basically expanded forms of the requirement files, were themselves expanded to become test vector files for the logic simulator. The criteria in the criteria files were used as the basis for the test vectors.

4.3.6 Verification

The calculation of test vector expected results was performed and independently verified by a person not involved in the design. The results of the simulation were written to waveform output files. These files were then used as input for a custom computer program that modeled the operation of the chip and independently calculated the results of each operation. The simulation output was then compared to the internally generated results, and any differences between the expected result (from the computer model) and the actual result (from the logic simulation) were flagged for further analysis. Notes were provided in the test files to explain differences in the results between the simulation waveform files and the chip model output files. The independent verification provided reasonable assurance that other errors (similar to the Multiplier/Diver error) do not exist.

4.3.7 Results

The tests were divided into three separate categories; with one category for each specification (requirements) document. The results for each are described in Reference 4.8.17. The Multiplier/Divider error that was discovered during integration testing was detected numerous times in the test. No other errors were found in the Multiplier/Divider or other functional modules of the ASIC.

4.4 DESIGN VALIDATION PROCESS

The design validation process was a two-step process. The first step was to validate the ASIC chip itself. The second step was to validate the ASIC chip mounted on the Main Board with all Personality Modules.

4.4.1 ASIC Test Approach

The ASICs were tested using an IMS model ATS1 integrated circuit tester. Both a wafer and package part test program was created. The wafer test program uses basic parametric screens and the functional test vectors only at nominal operating conditions. Die are packaged based on passing the wafer test. Packaged parts are subjected to both the functional and fault vectors. Packaged parts are tested at temperature and power supply extremes at higher than rated speed. The parts are also fully screened for parametrics, such as input voltage thresholds and leakage currents and output voltage levels and drive currents, etc.

4.4.2 Analysis of Test Coverage

The suite of test vectors used to screen the ASICs was designed to both prove performance and to reject parts with manufacturing flaws. Common failure mechanisms for digital ASICs are stuck-at faults, bridging faults, and speed faults. A stuck-at fault is where a node remains at the same value regardless of its proper value. Stuck-at faults can be caused by a short between a node and a power supply or an open circuit in an interconnect layer. Bridging faults are where two independent nodes always have the same value. Bridging faults are commonly caused by a short circuit in an interconnect layer or a failure of an isolating diode or insulator. Speed faults can be caused by process parametric variations that make a marginal path fail or by a thin interconnect, that adds an unmodelled parasitic resistance and corresponding increase in signal propagation delay through the interconnect.

There are many different potential failure mechanisms for an ASIC. However, studies have shown that even if a specific fault mechanism is not tested, it is extremely likely that it will be detected in a test that is geared toward a stuck-at mechanism. Parametric, as well as functional, operation is completely tested for each ASIC input, output and bi-directional pin. Every operation code is exercised including all possible no-operation codes. This approach tests every possible function of each of the functional blocks; i.e., Multi-Functional Adder, Multiplier/Divider, Square Root, Comparator, Analog-to-Digital Converter Interface, Digital-to-Analog Converter Interface, and Counter. Every on-chip Register is loaded with multiple patterns, and the Register outputs are transferred to ASIC output pins. Every data transfer path is exercised. All possible states of the program counter are tested. The non-obtrusive Monitor Bus is used to observe critical internal nodes during chip operation.

Speed faults are identified by operating the ASIC at greater than the rated clock speed during test and sampling outputs sooner after the clock than they will be required. The only critical external timing loops are from the clock to the address counter output, through the external memories, and back to the ASIC inputs. Adequate setup margin is verified by offsetting the

timing of inputs versus the system clock. Hold time is not an issue because of off-phase clocking of the data inputs and the delay of the address counter circuit and I/O.

There are two sets of test vectors for the ASIC—functional vectors and fault vectors. The functional vectors were created primarily to prove that a properly fabricated ASIC will perform as expected. Simulations were run and waveforms analyzed by ORNL. Using a simulator, the results at all internal nodes as well as chip inputs and outputs can be monitored. These simulations were converted to test vectors, which include only input patterns and expected results at the chip output pins. While the functional vectors were fairly comprehensive, there was no special effort to assure that changes in the state of internal nodes was reflected as a change to an output pin. Therefore a chip with internal flaws could pass the functional vectors. To supplement the functional vectors, a second set of vectors called fault vectors was created. The fault vectors paralleled the functional vectors but were much more comprehensive and took extensive advantage of the Monitor Bus. Additional operations were also added to transfer data from internal registers to output pins to further improve fault detection.

The Monitor Bus output goes directly to ASIC pins so continuous direct observation is possible. Data fed to the Monitor Bus includes both data words and control signals. The Monitor Bus operation is asynchronous, non-obtrusive and totally independent of normal circuit operation. This allows observation of as many monitor points as necessary during each clock cycle. This technique, stopping the chip clock and observing several monitor points before continuing, was used throughout the fault vectors.

The ASIC chip component successfully passed all original testing (Reference 4.8.21) and re-testing with enhanced functional and fault test vectors (Reference 4.8.22). These tests provide assurance that the manufactured ASIC chip has no manufacturing flaws and is performing as intended.

4.4.3 Integration Testing

In accordance with the Design, Verification and Validation Plan, Westinghouse was responsible for integration testing. Integration testing was performed with the ASIC chip mounted on the Main Board. All combinations of Main Board and Personality Modules were tested. It was during integration testing that the design flaw in the Multiplier/Divider functional module was discovered. Reference 4.8.16 describes the ASIC Multiplier/Divider error. The error was traceable to the ORNL design verification process. As described in paragraph 4.3.1, the functional test vector results were not independently verified. ORNL used the design simulation output to predict the expected results of the actual chip. Since the design simulation contained the same flaw as the chip, the expected results from the simulation test matched the actual results from the chip test. As part of the vector verification effort described in paragraph 4.3.6, all functional and fault test vector expected results were independently computed and verified by a person not involved in the original design. When the enhanced functional and fault test vector set was run on the design simulation and actual chip, the Multiplier/Divider flaw was detected. No other errors were detected in the Multiplier/Divider, and no other errors were detected in the other seven functional modules. This provided confidence that no other errors exist in the chip design.

The detection of the Multiplier/Divider error during the integration test phase of the program proved the concept that the ASIC chip design is simple and that testing can detect design or manufacturing issues.

4.5 FAULT GRADING

4.5.1 Introduction

Per NRC request, a fault grading analysis was performed on the ASIC. Fault testing is done to determine if any manufacturing flaws exist in fabricated ASICs. The software tools IFSIM and IRSIM were used to perform the fault grading of the ASIC. Vectors used in the fault grading tests were developed from the IRSIM model of the ASIC. The IFSIM software model of the ASIC provided statistical data on faults detected in the ASIC. IRSIM tests were done to exercise every control code in the chip layout. The test vectors developed for fault grading were applied to the ASICs. The functional test vectors developed for functional testing of the ASIC were combined with the fault vectors for a final set of vectors applied to the fabricated ASICs.

IFSIM is a software tool designed to do fault grading, and IRSIM is a software tool designed to simulate the detailed circuit operation of the ASIC. IFSIM uses much of the same software tools as IRSIM, but IFSIM does not simply run a single vector and provide a result. The inputs and outputs are defined and input vectors are selected for the fault-grade tests in IFSIM. IFSIM then faults each node in the ASIC high and low, runs the input vectors, and determines if the fault can be detected at the outputs. IFSIM first runs an input vector without a fault to determine what the correct output should be. It then faults a node and compares the correct output to the output with a fault. If the outputs are different, it declares the fault detected. If the outputs are the same or if the faulted output is undetermined, then the faulted node is declared as undetected. IFSIM faults each node high and low. Therefore, each node is tested twice—once low and once high. The number of nodes listed by IFSIM is actually twice the actual number of nodes in the circuits.

Because IFSIM uses a transistor-level model of the ASIC and it can be made to fault every node in the ASIC, a large ASIC cannot be fault graded in a reasonable time with this tool. Therefore, the ASIC was separated into the eight smaller functional module circuits for testing.

4.5.2 Measured Fault Analysis Percentages

The fault analysis percentages were calculated for each of the eight circuits evaluated. The details of the results of the fault analysis are contained in Reference 4.8.18. The percentage was calculated using the following equation:

Fault analysis (%) = [(Total nodes - unanalyzed nodes)/(Total nodes)] * 100%

Where:

Total nodes is the number of nodes analyzed by IFSIM, which is twice the number of nodes in the circuits,

Unanalyzed nodes are the nodes that were not detected by testing and were not removed from the fault analysis undetected list by analysis.

Based on this equation, the fault analysis percentages were calculated to be the following. The Registers have 100.0 % fault analysis with no unanalyzed nodes out of 4798 nodes. The MFA has 100.0 % fault analysis with no unanalyzed nodes out of 5122 nodes. The Multiplier/Divider fault analysis is 99.4 % with 27 unanalyzed nodes out of 4688. The Square Root fault analysis is 99.3 % with 29 unanalyzed nodes out of 4424. The Comparator fault analysis is 100.0 % with no unanalyzed nodes out of 8906. The DAC Interface fault analysis is 100.0 % with no unanalyzed nodes out of 1774. The ADC Interface fault analysis is 99.9 % with 2 unanalyzed nodes out of 3510. Fault analysis for the chip Counter is not being calculated in IFSIM or IRSIM as explained below. A summary of the results for the fault analysis is given in Table 4-1.

TABLE 4-1

FAULT ANALYSIS SUMMARY

Circuit	Number Of Nodes	Covered Nodes	Percent Covered
Registers	4798	4798	100.0 %
MFA	5122	5122	100.0 %
Mult/Div	4688	4661	99.4 %
Square Root	4424	4395	99.3 %
Comparator	8906	8906	100.0 %
DAC	1774	1774	100.0 %
ADC	3510	3508	99.9 %
Total	33222	33164	99.8 %

IRSIM and IFSIM identify the transistor nodes in the circuits by alphanumeric characters assigned by the computer. For some nodes, this identifier (ID) cannot be used to locate precisely where the node is in the circuit. However, many of the undetected nodes can be located by using a combination of node ID, gate type, and connections to other gates. This approach was used to determine the location of all nodes as being in control circuits or in functional circuits. In many cases the nodes were located precisely in a circuit; in other cases it was determined that a node was one of several in a group of identical circuits. Although the location of some of the nodes was not determined precisely, they were located closely enough to determine whether they were control or functional circuits. The control circuits decode the controller commands and select functional circuits. The functional circuits do mathematical operations or manipulate data. The undetected nodes were separated into control nodes and functional nodes.

The control nodes could not be tested completely with the IFSIM fault grader because the circuits being tested were only part of the entire ASIC. For example, some control commands access circuits that were not part of the circuit under test. Because the ASIC was separated for testing purposes, it was not possible for the separated circuits to communicate with one another. Therefore communication between the individual circuits was simulated in IFSIM, but this simulation of un-represented circuits would not be useful for testing the ASIC. However, all the control nodes can be tested by issuing all the control codes to the ASIC (all the circuits combined). This cannot be done in IRSIM or IFSIM, but it can be done on the actual chip. Because all 256 control codes can be issued and input jumpers set, it is logical to conclude that all the control circuits can be tested.

There are also some nodes in the ASIC that were eliminated from the undetected list because they were connected to the voltage supply or to ground, such as pull-up or pull-down nodes, and not driven by other circuits. These nodes in the ASIC are connected through a resistor to ground or to +5 volts. A node that is connected to ground will not be detected as failing low because it is always low. If IFSIM simulates a ground fault on a grounded node, the output is always correct and the node would be declared uncovered. Likewise, a node connected to 5 volts would be declared as uncovered for faults to 5 volts. However, because the circuit is designed with these nodes connected to ground or to the voltage supply, they should not be considered uncovered by the fault grader. Therefore, the nodes that could be identified as always low or always high were removed from the IFSIM "failed" list for calculation of coverage.

4.5.3 Discussion of Fault Analysis

Nodes in each circuit were detected as covered for faults by using IFSIM and IRSIM. After these simulation tests were completed there were some nodes that were faulted but could not be detected by these programs. Pull-up and pull-down circuits were analyzed to show that they would not fail low for pull-down or high for pull-up because they were permanently connected low or high. Similar analyses were applied to other circuits, such as tri-stated buffer circuits. Many of the tri-state failures were in tri-states used to output data to the Monitor Bus. However, none of the tri-state faults would cause a failure in functional circuits because transistors in the other tri-state circuits isolated them.

All of the undetected faults in the tri-state circuits, except those used in the Counter circuits (the Counter circuits are analyzed separately), were faulted as though the circuit were not enabled (floating). Therefore, they would affect the Monitor Bus only when they were floating. For these tri-states to output an incorrect value while the tri-state was floating would result in an additional fault in the tri-state. Multiple faults would be required for the tri-state fault to possibly affect the test results. This potential interaction which would affect circuit testing, only would occur if the tri-state outputs a value onto the Monitor Bus when it should have been floating and another tri-state did not output the correct value when enabled at the same time If the value output by the faulted tri-state were the correct value for the other circuit, then the fault analysis would not detect either fault. Because multiple faults are required, the faults must interact in particular ways, and that neither fault would be detected by other tests, the Monitor Bus tri-state faults were not included in the unanalyzed lists.

Another method of concluding that the circuits can be removed from the undetected fault list is through a logical argument that all feasible inputs are input to the circuit. This applies to the control nodes in each functional circuit and to the ASIC controller interface circuits. There are eight bits in the controller, which can generate 256 possible control commands. These commands were generated in both the functional test vectors and in the fault grade test vectors.

4.5.4 Control Node Tests

All the control codes were issued as part of the functional tests using a technique to ensure that no control code would interfere with another control code. This technique was to issue all the control codes that do not affect the circuits being analyzed, and then to issue the remaining control codes that affect or operate on the circuits being evaluated. Because these control codes were all issued as part of the functional tests, they are not reissued in the fault grade tests.

4.6 COMMERCIAL DEDICATION

A commercial dedication process was followed for fabrication of the actual ASIC chip. The commercial dedication is based on the fact that the design of the ASIC is simple, the chip and functions are thoroughly testable, and the Qualification and Validation Test Programs demonstrated that the chip performs as intended in safety-related functions.

The Commercial Dedication process was performed in accordance with Reference 4.8.10. Reference 4.8.12 is the Commercial Grade Survey Plan and Report for the chip foundry, Northrop Grumman ATC. The Commercial Grade Survey was performed by reviewing the ATC Quality Assurance Manual, Product Specification Abbreviated Form (PSAF) for the ASIC mask set 4457, non-Westinghouse related and Westinghouse specific Trip Tickets as well as supporting procedures and records. In addition, interviews were conducted at the office and/or workstations of personnel performing activities associated with critical characteristics. The Commercial Dedication Instruction, Reference 4.8.11, contained the critical characteristics. The critical characteristics were derived from the design requirements, specifications, and chip drawing, Reference 4.8.9.

The applicable quality assurance program aspects of ATC in place during the survey were found to be effectively controlled as they relate to Westinghouse established critical characteristics. In summary, all areas of the survey were found to be satisfactory and in compliance with the ATC QA program. As a result, ATC was placed on the Westinghouse Qualified Supplier List.

At the component level, all ASIC chips are factory acceptance tested with a combination of Functional Test Vectors, Fault Test Vectors and MIL-STD-883 Burn-In for 160 hours at 125 °C minimum. Component reliability is achieved by selecting a reliable manufacturing process. The ATC fabrication process is documented on the ASIC chip drawing, Reference 4.8.9. The ASIC chip is made from a mask set, Reference 4.8.8. Any design changes would require a new mask set.

The ASIC chip is mounted on the Main Board along with all other components that comprise the ABRM. The Main Board and Personality Modules were subjected to a series of qualification tests. These tests consisted of Environmental, Seismic, EMC and Fault Qualification Tests. The ABRM successfully passed all qualification tests. The ABRM Validation Test Program (which included Abnormal Conditions and Events tests) demonstrated that the ASIC chip performed as intended for all module level process functions.

The Qualification and Validation Test Programs demonstrated that an ASIC chip that passes the factory acceptance test program will perform as intended in its safety-related function(s). This provides assurance that all chips that pass the factory acceptance test program are acceptable for use in the ABRM. Any failure after manufacture is a single random hardware failure, and not a common-mode failure.

4.7 CONCLUSION

The design, testing and commercial dedication features identified herein and summarized below provide adequate assurance that the ASIC chip that passes the factory acceptance test contains no manufacturing flaws and will perform as intended in its safety-related function(s).

Failure modes of the ASIC chip have been analyzed and are detectable by normal surveillance testing. When installed on the Main Board with a Personality Module, any failure of the ASIC chip will manifest itself as an incorrect or inaccurate analog output value, or a discontinuity in the output waveform. No new failure modes are introduced by using the ASIC-Based Replacement Module.

Summary of Design Features

- Design, Verification and Validation Plan defined the process that was followed throughout.
- Functional requirements and specifications were created that identified requirements for safety system applications.
- Chip design consists of simple math functions that are easily tested.
- Chip contains only functional modules required to implement process functions, no other functions.
- Functional modules are hardwired.
- Chip was designed and tested from bottom-up.
- Industry standard libraries used for primitive cell structures.
- Chip operation is entirely deterministic:

- No system latch-up.
- No undefined states.
- No interrupts.
- No loops or branching.
- No decisions are based on measured data or results.
- Each step is defined and repeated continuously in a loop.

- Monitor Bus incorporated into design to increase fault coverage.

Summary of Test Features

- Functional modules are thoroughly testable.
- Functional modules can be tested independently of each other.
- Design testing:
  - Design simulation tested by ORNL.
  - Design simulation test repeated by ATC.
  - Prototype chips fabricated by ORBIT and tested by ATC. Results matched simulation test results.
  - Production chips fabricated by ATC and tested with original test vector set. Results matched simulation test results.
  - All test results were compared to each other for accuracy and reproducibility (matched).
  - Production chips re-tested by ATC with enhanced functional and fault test vector set.
- Enhanced Functional and Fault Test Vector Set:
  - Exercises 99.8% of gates on chip (4 circuits have 100% coverage).
  - Developed from functional decomposition of design requirements.
  - Expected results independently computed and verified by person not involved in design.

- Detected Multiplier/Divider error.
- Provides reasonable assurance that manufactured chip has no manufacturing flaws and is performing as intended.

- Chip failures detectable as evidenced by Multiplier/Divider error discovered during integration testing.

Summary of Commercial Dedication Features

- Commercial Dedication Process:
  - Performed in accordance with Westinghouse Quality Assurance Program.
  - Chip vendor (ATC) placed on Westinghouse Qualified Supplier List.
  - Reliable manufacturing process used and documented for repeatability.
- Critical characteristics derived from the design requirements, specifications and chip documentation.
- Factory Acceptance Test consists of:
  - Functional Test Vectors.
  - Fault Test Vectors.
  - MIL-STD-883 Burn-In for 160 hours at 125 °C.
  - Every device is tested.
- Qualification and Validation Test Programs (which included ACE's testing) demonstrated that an ASIC chip that passes the factory acceptance test program will perform as intended in its safety related function.
- Dedication basis is maintained because any design change would require a new mask set.
- Any failure after manufacture is a single random hardware failure, and not a common mode failure.

4.8 REFERENCES AND DOCUMENTATION LIST

4.8.1 WOG Letter OG-97-069, dated 7/10/97, Initial Submittal of Application Specific Integrated Circuit (ASIC) Design Information.

4.8.2 Westinghouse Specification 413A63, Revision 0, ABRM Main Board and Personality Module Design Specification.

4.8.3 Westinghouse Specification 413A66, Revision 0, ASIC Design Specification.

4.8.4 Westinghouse Specification 413A67, Revision 0, ASIC Interface Specification.

4.8.5 Westinghouse Specification 413A69, Revision 0, ASIC Functional Description.

4.8.6 ASIC Functional Decomposition Matrix, 1/22/98.

4.8.7 ORNL ViewLogic File, ASIC schematic.

4.8.8 ATC Manufacturing Part Number/ASIC Mask Set 4457.

4.8.9 Westinghouse Drawing 2A10000, Revision 1, 7300A ASIC-Microcircuit, Digital, CMOS, VLSI, Standard Cell, Macro-Cell Specifications.

4.8.10 WCAP-12885, Revision 0, Westinghouse Nuclear Services Division Commercial Dedication Program.

4.8.11 Westinghouse Commercial Dedication Instruction (CDI), Number SEP-0662, 2/17/97.

4.8.12 Westinghouse Commercial Grade Survey Plan and Report for Northrop Grumman ASIC Chip, WES-97-172, 6/6/97.

4.8.13 ORNL Paper "Test and Verification of a Reactor Protection System Application Specific Integrated Circuit," 12/18/96.

4.8.14 ORNL Report, "Reactor Protection System (RPS) Functional Test Report," 1/14/97.

4.8.15 ORNL Report, "Reactor Protection System (RPS) Fault Coverage Test Vectors," Revision 1, 6/30/97.

4.8.16 ORNL Report, "ASIC Divider Error," 10/2/97.

4.8.17 ORNL Report, "Functional Testing of the RPS ASIC," 12/4/98.

4.8.18 ORNL Report, "Fault Grading of the RPS ASIC," 2/2/99.

4.8.19 ATC Design Test Report, "Northrop Grumman ATC Test of ORNL 7300A ASIC Design," 10/28/97.

4.8.20 ATC Prototype Test Report, "Northrop Grumman ATC Test of Orbit Semiconductor Fabricated 7300A ASIC," 10/28/97.

4.8.21 ATC Production Test Report, "Northrop Grumman ATC Test of Production 7300A ASICs," 6/30/97.

4.8.22 ATC Functional and Fault Test Report, "Report on Functional and Fault Vector Testing of Sixty-Six 2A10000 Units per PO SAMB38792H, Change Notice 005," 1/19/00.

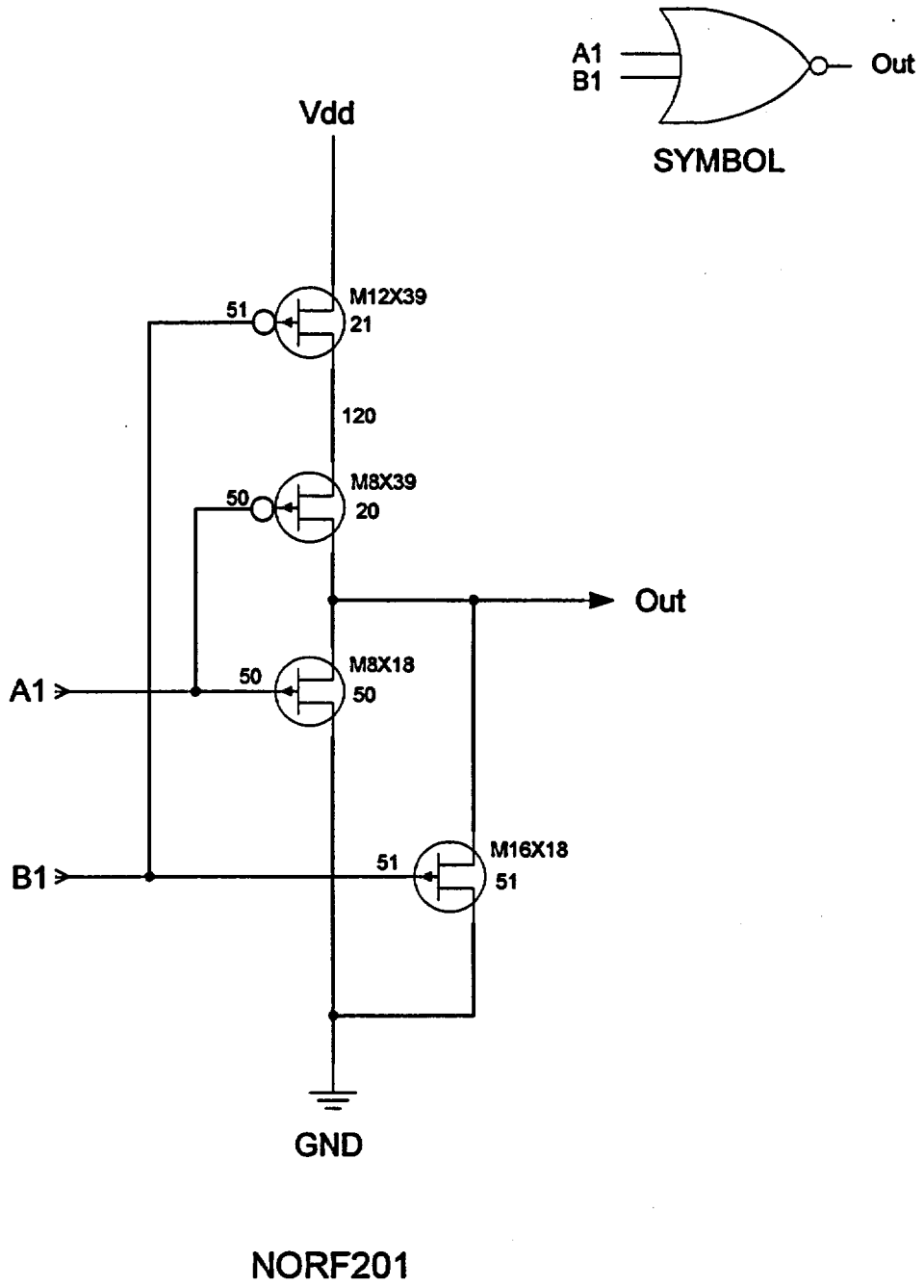
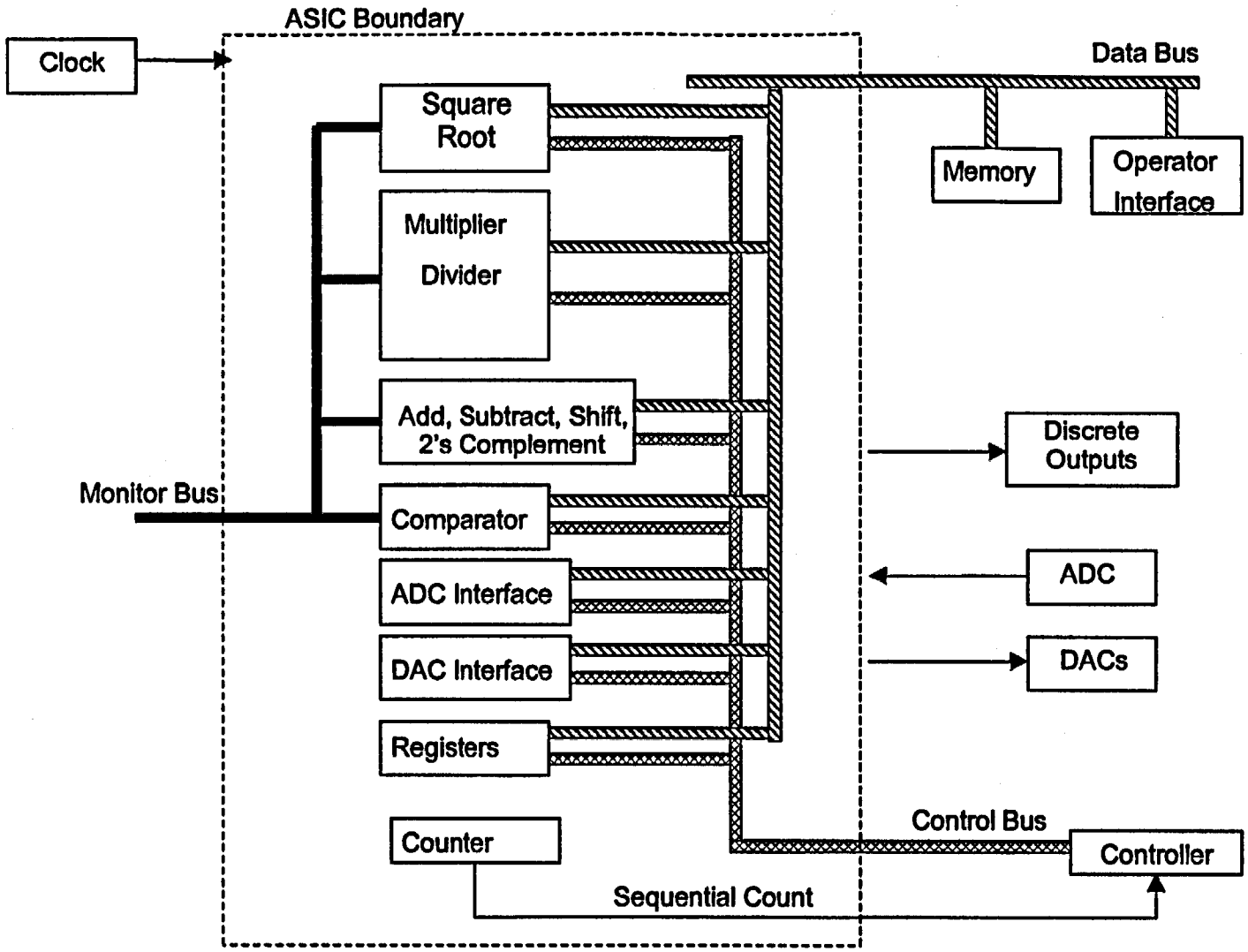


FIGURE 4-1 NOR GATE PRIMITIVE CELL



DAC: Digital-to-Analog Converter
ADC: Analog-to-Digital Converter

FIGURE 4-2 ASIC FUNCTIONAL BLOCK DIAGRAM

5.0 VALIDATION TEST PROGRAM

5.1 VALIDATION TESTING OVERVIEW

In accordance with the ABRM Design, Verification and Validation Plan (413A62), a Validation Test Plan was generated. The ABRM Validation Test Plan defined a methodology that must be followed to perform a series of functional requirement based tests which compliment the reviews and simulations conducted during the design verification phase. The ABRM Validation Test Plan was submitted to the NRC for review via Reference 5.6.1.

During design verification, a bottom-up approach was used to thoroughly and individually review and/or simulate each major "application" or portion of the overall design. This approach verifies that each element operates properly as a stand-alone entity.

Validation testing complements the design verification process and ensures that the final implemented design satisfies the top-level functional requirements and that acceptable engineering practice was utilized during the design and implementation of the system. This process was accomplished by conducting three independent types of validation tests on each ABRM module type,

(1) Functional Requirements Testing - this testing ensured that the design met the functional requirements and that acceptable engineering practice was utilized in the design and implementation of critical areas of the system. The items covered within this section required the internals of the system design and implementation to be analyzed in detail. Included in this section is thorough testing of the Operator Interface used to enter, change and store setpoints and tuning constants.

(2) Qualification Testing - this testing ensured that the design operates within predefined acceptance criteria when subjected to anticipated extremes of the environment, seismic disturbances and electrical interference.

(3) Abnormal Conditions and Events (ACEs) Testing - this testing ensured that the design operates in a known and predictable manner under abnormal-mode conditions.

Functional Requirement Testing and Qualification Testing treat each module as a black box while the Abnormal Conditions and Events Testing requires that the internal structure of the module design be analyzed in detail. Due to this dual approach, validation testing provides a level of thoroughness and testing accuracy which is at least equivalent to that which occurs during design verification, and ensures detection of any deficiencies that occurred during the design process but were not discovered during design verification. Validation testing is performed on the verified design using the final target hardware, which includes the:

- NXX Main Board;
- 14 Personality Modules; and

- 29 Controller Algorithms.

5.2 FUNCTIONAL REQUIREMENTS TESTING

The functional requirements generated during the requirements phase served as the basis for identifying the tests that must be conducted. This activity consisted of decomposing the functional requirement documents into extensive test procedures to be followed during validation testing. The process ensured that the design meets the functional requirements.

Validation Test Procedures were generated for each of the fourteen ABRM configurations. The Validation Test Procedures are detailed instructions that demonstrate that the ABRM operates in accordance with the:

- ABRM Main Board and Personality Module Design Specification (413A63);
- Operator Interface Design Specification (413A64);
- 7300 Analog Product Verification Test Reports; and
- 7300 Analog Instruction Bulletins.

The Validation Test Program was designed to demonstrate the suitability of the ABRM module to function as a direct replacement for the analog module and ensure that acceptable engineering practice was followed during the design. Validation testing addressed the following critical design areas.

(1) Time response tests.

(2) Analog output signal accuracy tests at both normal and abnormal temperature and humidity conditions and at DC power supply voltage extremes.

(3) For the NAL and NAC applications, trip point accuracy tests at both normal and abnormal temperature and humidity conditions and at DC power supply voltage extremes.

(4) Dynamic response performance tests for ABRM applications that perform time dependent functions (such as lead/lag).

(5) Overload and recovery tests to establish ABRM output signal response to an input signal over-range condition.

(6) Analog output signal noise tests to establish acceptability of output signal noise levels.

(7) Power dissipation and inrush current tests to establish full load power dissipation and inrush levels.

(8) Module interaction tests to detect any adverse affects caused by installing an ABRM adjacent to an analog module.

(9) Interfaces between other systems, subsystems or components.

(10) Maintenance and calibration features, including test points.

(11) Diagnostics and alarms.

(12) Component placement for manufacturability.

(13) Location of operator interface controls.

(14) Ability to configure all groups.

(15) Verification of drawings.

For the Operator Interface, the following critical elements are checked to ensure proper system operation:

(1) System is capable of accepting all information, as required by the application, to be entered by a human.

(2) All setpoints and tuning constants required by the function can be entered and stored.

(3) All manually entered voltage values are scalable to the proper engineering units (gpm, seconds, etc).

(4) Memory retention requirements are correctly implemented (i.e., no battery back-up, storage of intermediate values, etc.).

(5) Design does not permit abnormal data entries (i.e., out of range, improper order, etc.).

(6) Sufficient precautions are provided to prohibit the operator from inadvertently introducing unintended functions (i.e., improperly configure the system).

(7) The human-machine interface operates as defined in the requirements (i.e., unambiguous indications, human factor considerations, etc.).

Most of these items do not relate directly to a functional requirement or to a series of functional requirements, but address system integrity defined during the requirements and design phases. Reviewing/testing the design against these criteria provides assurance that the design and interface requirements have been implemented in such a manner that undesirable interactions will not occur.

5.3 QUALIFICATION TESTING

During this phase of validation testing, the hardware is tested under the expected extremes of environmental conditions, seismic stresses and electrical interference. Typical qualification tests include the following:

(1) Environmental (temperature and humidity);

(2) Seismic;

(3) Electro-Magnetic Compatibility (Emissions, Susceptibility, Surge, Fast Transient); and

(4) Electrical Fault.

Refer to Section 6 of this report for a summary of the Qualification Test Program.

5.4 ABNORMAL CONDITIONS AND EVENTS TESTING

During this phase of Validation testing, the functional requirements were reviewed to define a series of abnormal conditions under which the system must operate properly without causing any inadvertent or detrimental actions. Examples of abnormal-mode tests include division by zero, input signal over-range and recovery, and incorrect setpoints/tuning constants. ACEs testing was incorporated into the Validation Test Procedure for each ABRM module.

Abnormal Conditions and Events testing demonstrated that the ABRM module operated in a known and predictable manner for abnormal signals, setpoints, tuning constants and configurations. The modules were tested for input signals that were out of range and/or the wrong polarity. Setpoints and tuning constants were set out of range, and jumper configurations were set incorrectly, to simulate technician error. In all cases, the ABRM performed as expected, and the malfunction was detectable during bench calibration or normal surveillance testing.

5.5 CONCLUSION

The ABRM Validation Test Program demonstrated that the ABRM meets the performance requirements of the equivalent analog module it replaces, and that the sequence of operations defined in the Controller algorithm correctly implements the desired process function.

At the completion of the Validation Test Procedure for each ABRM module type, the test results are summarized in a module specific Validation Test Report. The results of the validation testing demonstrated that the system design meets the system functional requirements.

5.6 REFERENCES

5.6.1 WOG Letter WOG-ASIC-00-004, dated 1/27/00, Fourth Submittal of Application Specific Integrated Circuit (ASIC) Design Information.

6.0 QUALIFICATION TESTING

During this phase of testing, the hardware was tested under the expected extremes of environmental conditions, seismic stresses and electrical interference. The Qualification Test Program included the following tests:

(1) Environmental Qualification (temperature and humidity extremes);

(2) Seismic Qualification;

(3) Electromagnetic Compatibility (Emissions, Susceptibility, Fast Transient and Surge); and

(4) Electrical Fault Qualification.

Qualification testing was performed in accordance with the following process.

(1) Functional Requirements Decomposition: The top-level functional requirements were reviewed to identify detailed qualification requirements. The type of test that must be conducted to exercise the system under each specified qualification condition was defined.

(2) Qualification Test Procedure Generation: Once the decomposition was complete, the specifics of the test(s) were defined in test procedural form such that they can be conducted during qualification testing.

(3) Qualification Test Execution: The detailed tests were conducted in accordance with the qualification test procedures and the results were reviewed by the design team.

6.1 ENVIRONMENTAL QUALIFICATION

The Environmental Qualification Program objective was to demonstrate that the ABRM meets specific performance requirements during exposure to abnormal environmental conditions when tested in accordance with Reference 6.5.1 and Reference 6.5.2.

6.1.1 Environmental Test Criteria

The ABRMs were installed in a 7300 System double card frame and subjected to abnormal environmental conditions, which simulated a temporary change in an internal 7300 cabinet environment. Cycle 1 testing combined the maximum temperature of 140 °F with a lower humidity and the maximum 7300 System power supply extreme of 27 Vdc. Cycle 2 testing combined the maximum relative humidity of 95 % with a lower temperature and the minimum 7300 System power supply extreme of 22 Vdc. The duration of each test cycle was 24 hours.

6.1.2 Environmental Test Acceptance Criteria

The environmental test acceptance criteria required the ABRMs to be completely operable during the abnormal environmental conditions. In addition, the following performance requirements had to be maintained with an analog output loading of 600 ohms.

- The output of the Delta_T/T_avg loop shall remain within 0.5 % of span.
- The outputs of any ABRM tested individually shall not exceed 0.1 % of span per 50 °F change in ambient conditions.
- The outputs of the control loops shall remain within 0.5 % of span.

6.1.3 Environmental Test Configuration

The environmental test configuration exercised three of each component used in the design of the ABRM. To ensure that all modules and components were represented, the test configuration consisted of 30 ABRMs mounted in a 7300 System double card frame and arranged as follows:

- 16 ABRMs arranged as a Delta T/Tavg protection loop;
- 6 ABRMs arranged in three control loops; and
- 8 ABRMs arranged as stand-alone modules.

6.1.4 Environmental Test Results

As documented in Reference 6.5.3, the ABRM successfully completed environmental qualification testing. The anomalies observed during the environmental testing are discussed in the test report. Based on the successful completion of the tests on the Main Board and all Personality Modules, it was concluded that the ABRM performance during the abnormal environmental conditions is acceptable and meets the requirements of Reference 6.5.1. The temperature coefficient for the NRA module has been relaxed from 0.1 % per 50 °F to 0.25 % per 50 °F to allow for some drift in the analog input signal conditioning circuitry. The minimum loading for any analog output from an ABRM is 600 ohms. The NCB module performance is defined by the testing but it must be evaluated for acceptability based on the system application.

The ABRM Environmental Test Report, Reference 6.5.3, was submitted to the NRC for review via Reference 6.5.4.

6.2 SEISMIC QUALIFICATION

The Seismic Qualification Program objective was to demonstrate that the ABRM meets the performance requirements before and after simulated seismic service conditions when tested in accordance with Reference 6.5.5.

6.2.1 Seismic Test Criteria

The ABRMs were subjected to equal and simultaneous inputs in the front-to-back, side-to-side and vertical directions. The test input was random excitation, 30 seconds in duration. The test input included frequency content up to 33 Hz and all requirements specified in Reference 6.5.5. The Operating Basis Earthquake (OBE) is 2/3 the Safe Shutdown Earthquake (SSE) seismic level for all principal directions. The SSE in the vertical direction is 2/3 of the horizontal direction.

6.2.2 Seismic Test Acceptance Criteria

The seismic test acceptance criteria specified that the ABRMs maintain the following performance requirements.

- All outputs shall maintain steady-state conditions following each test run. Any deviations during or following the test run must be evaluated.
- All outputs must maintain continuity during all test runs.
- All bistables shall change state when inputs exceed trip points.

6.2.3 Seismic Test Configuration

The seismic test configuration exercised three of each component used in the design of the ABRM. To ensure that all modules and components were represented, the test configuration consisted of 30 ABRMs mounted in a 7300 System double card frame and arranged as follows:

- 16 ABRMs arranged as a Delta_T/T_avg protection loop;
- 6 ABRMs arranged in 3 control loops; and
- ABRMs arranged as stand-alone modules.

6.2.4 Seismic Test Results

As documented in Reference 6.5.6, the ABRMs successfully completed seismic testing. No anomalies attributable to the seismic testing were observed other than the fatigue issues discussed in the test report. Based on the successful completion of the tests on the Main Board and all Personality Modules, it is concluded that the ABRM is seismically qualified in accordance with the requirements of Reference 6.5.5 to the levels defined in the report.

The ABRM Seismic Test Report, Reference 6.5.6, was submitted to the NRC for review via Reference 6.5.7.

6.3 ELECTROMAGNETIC COMPATIBILITY (EMC)

6.3.1 EMC Test Criteria

The ABRMs were tested in accordance with Reference 6.5.8.

6.3.2 EMC Test Acceptance Criteria

For emissions, radiated and conducted, the ABRMs shall be less than the levels identified in Reference 6.5.8.

For susceptibility, radiated and conducted, the NAL and NAC ABRMs shall not exhibit spurious trips, and these modules must trip on demand. For the other ABRMs, a change greater than 25 mV deviation on the analog output was established as a threshold guideline that would require evaluation, or the analog output deviation shall be less than the equivalent 7300 analog module.

For surge and electrical fast transients, the ABRMs must recover to normal operation and accuracy after the transient. There shall be no permanent degradation.

6.3.3 EMC Test Configuration

Individual ABRMs were mounted in a 7300 System double card frame using standard mounting hardware. The card frame was powered from a standard 7300 System cabinet power supply. Input and output cables were attached to the card edge connectors to simulate internal cabinet wiring. When required for comparison, the ABRM was removed from the card frame and the equivalent analog module installed and the test repeated.

6.3.4 EMC Test Results

As documented in Reference 6.5.9, the ABRM radiated emissions were less than the allowable equipment limits per Reference 6.5.8. Conducted emissions were also less than the allowable equipment limits except at one frequency which exceeded the limit but still exhibited considerable margin with respect to the allowable plant level.

The ABRM susceptibility (radiated and conducted) test results were generally the same as or better than the equivalent 7300 Series analog module. All cards demonstrated acceptable results at a minimum of 8 dB margin over the measured plant emission data contained in Reference 6.5.8.

For the surge and electrical fast transient testing, all ABRMs returned to initial conditions after application of the transient.

The ABRM EMC Test Report, Reference 6.5.9, was submitted to the NRC for review via Reference 6.5.10.

6.4 FAULT QUALIFICATION

The objective of the Fault Qualification Program was to demonstrate that the NLP and NSC ABRMs meet the performance requirements when subjected to various fault conditions on isolated outputs that interface with non-Class 1E circuits.

6.4.1 Fault Test Criteria

The ABRM fault tests included short circuits, applied common mode fault voltages, and line-to-line transverse mode fault voltages. Direct current voltages were applied in both positive and negative polarities. The fault voltages were:

- 125 VAC_{rms}, 60 Hz;
- 580 VAC_{rms}, 60 Hz;
- 125 VDC; and
- 250 VDC.

These test conditions are the same as applied to the original 7300 System analog modules, Reference 6.5.11.

6.4.2 Fault Test Acceptance Criteria

The fault test acceptance criteria required that the NLP and NSC ABRMs maintain the following performance requirements.

- The modules shall maintain the ability to perform protective functions before, during and after the application of the fault condition.
- Any resultant solder or circuit board component splatter shall be evaluated to determine if it could adversely affect an adjacent ABRM or other components on the same circuit board.

6.4.3 Fault Test Configuration

The fault test configuration consisted of an NLP Voltage-to-Voltage Isolator and an NSC Voltage-to-Current Isolator mounted in a typical 7300 System card frame with input and output cables attached. Fault conditions were applied to the isolated outputs.

6.4.4 Fault Test Results

As documented in Reference 6.5.12, the NLP and NSC ABRMs successfully completed fault testing. No anomalies attributable to the fault testing were observed other than the issues described in the Test Report. Based on the successful completion of the tests on the Main Board and the NLP and NSC Personality Modules, as described in the report and with the modifications developed, it is concluded that the ABRM has been shown to be in compliance with the isolation capabilities described in Reference 6.5.13.

The ABRM Fault Conditions Test Report, Reference 6.5.12, was submitted to the NRC for review via Reference 6.5.14.

6.5 REFERENCES

6.5.1 IEEE Std 323-1983, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations", Section 6.3.2(3).

6.5.2 Westinghouse WCAP-8587, Revision 6, "Methodology for Qualifying Westinghouse WRD Supplied NSSS Safety Related Electrical Equipment," March 1983.

6.5.3 Westinghouse WCAP-15378, Revision 0, "Environmental Test Report for Westinghouse ASIC-Based Replacement Module for 7300 Process Protection System," February 2000.

6.5.4 WOG Letter WOG-ASIC-00-007, dated March 6, 2000, "Sixth Submittal of Application Specific Integrated Circuit (ASIC) Design Information."

6.5.5 IEEE Std 344-1987, "IEEE Recommended Practices for the Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations."

6.5.6 Westinghouse WCAP-15215, Revision 0, "Seismic Test Report for Westinghouse ASIC-Based Replacement Module for 7300 Process Protection System," May 1999.

6.5.7 WOG Letter WOG-ASIC-99-019, dated August 9, 1999, "Third Submittal of Application Specific Integrated Circuit (ASIC) Design Information."

6.5.8 EPRI TR-102323, Revision 1, "Guidelines for Electromagnetic Interference Testing in Power Plants," January 1997.

6.5.9 Westinghouse WCAP-15403, Revision 0, "EMC Test Report for Westinghouse ASIC-Based Replacement Module for 7300 Process Protection System," April 2000.

6.5.10 WOG Letter WOG-ASIC-00-019, dated 5/12/00, "Seventh Submittal of Application Specific Integrated Circuit (ASIC) Design Information."

6.5.11 Westinghouse WCAP-8892A, "Westinghouse 7300 Series Process Control System Noise Tests," June 1977.

6.5.12 Westinghouse WCAP-15371, Revision 0, "Fault Conditions Test Report for Westinghouse ASIC-Based Replacement Module for 7300 Process Protection System," February 2000.

6.5.13 IEEE Std 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations", Section 5.6.3.1 (b).

6.5.14 WOG Letter WOG-ASIC-00-005, dated February 7, 2000, "Fifth Submittal of Application Specific Integrated Circuit (ASIC) Design Information."

7.0 RELIABILITY ASSESSMENT AND FAILURE MODES AND EFFECTS ANALYSIS

7.1 ABSTRACT

A Reliability Assessment Program was conducted to assess the card level reliability for the ASIC-Based Replacement Modules (ABRM) to be used as replacement cards for the Westinghouse 7300 System analog card styles. In support of this project goal, a Mean Time Between Failures (MTBF) parts count reliability assessment and Failure Modes and Effect Analysis (FMEA)/Functional Block Reliability Assessment were performed for the ABRM. Results of these analyses are provided in Reference 7.7.23 and are summarized as follows.

- The calculated MTBF for all fourteen of the ABRM NXX Main Board and Personality Modules exceeded the calculated MTBF for the equivalent 7300 analog card styles.
- All fourteen of the ABRM NXX Main Board and Personality Modules exceed the ASIC-Based NXX Design Specification value of 100,000 hours at 30 °C at the functional level.
- No new failure modes are created as a result of the application of the ABRM.

7.2 INTRODUCTION

The results of the card level reliability assessment for the ABRM is documented herein. This assessment has three purposes.

(1) To calculate the MTBF for the ASIC-Based Replacement Modules.

(2) To determine the failure modes and effects for the ABRMs.

(3) To provide a comparison between the ABRM NXX Main Board/Personality Module(s) and the 7300 Series analog system equipment targeted for replacement.

7.3 APPLICABLE RELIABILITY GUIDANCE STANDARDS AND ACRONYMS

7.3.1 Applicable Reliability Guidance Standards

(1) IEEE-603-1991 requires that reliability goals be established as part of the safety system design basis and that reliability assessments be performed to demonstrate that goals are met.

(2) IEEE-577-1976 and IEEE-352-1987 provide guidance for performing reliability assessments of Nuclear Plant safety systems.

(3) MIL-STD-1629A provides guidance for performing an FMEA.

7.3.2 ACRONYMS

ASIC	Application Specific Integrated Circuit
FBA	Functional Block Analysis
FMEA	Failure Modes and Effects Analysis
FP	Field Power
FPGA	Field Programmable Gate Array
G_B	Ground Benign Temperature (MIL-HDBK-217F standard term)
I/O	Input/Output
MB	Main Board
MTBF	Mean Time Between Failure
PM	Personality Module(s)
RAM	Random Access Memory

7.4 ANALYSIS SCOPE

The scope of this analysis includes the following equipment.

ASIC NXX Main Board

NAC Analog Comparator Personality Module

NAL Comparator Personality Module

NCB Controller Personality Module

NCD Controller Driver Personality Module

NCH Function Generator Personality Module

NLL Lead/Lag Personality Module

NLP Isolator and Loop Supply Personality Module

NMA Mixing Amplifier Personality Module

NMD Multiplier/Divider Personality Module

NRA RTD Amplifier Personality Module

NSA Summing Amplifier Personality Module

NSC Signal Converter Personality Module

NTD Tracking Driver Personality Module

NVP Voltage to Pulse Converter Personality Module

7.5 METHODOLOGY

7.5.1 Parts Count MTBF Calculations

7.5.1.1 Methodology

The failure rate calculations are based on the MIL-HDBK-217F Notice 1 and 2 parts count prediction method, or vendor data, where available. The parts count method is a conservative means for calculating MTBF as it provides a representative estimate of the MTBF that could be expected. The parts count method evaluates the total failure rate for a component by looking up a generic failure rate and quality factor in Appendix A of MIL-HDBK-217F. The failure rate that is obtained, is multiplied by a quality factor associated with that component type, and then summed with the failure rates obtained for other components used in the equipment. The general mathematical expression for equipment failure rate with this method is:

$$\lambda_{EQUIP} = \Sigma_{(\text{for } i=1 \text{ to } n)} N_i (\lambda_g \Pi_Q)_I$$

where:

λ_{EQUIP} = Total equipment failure rate (Failures/10^6 hours)

λ_g = Generic failure rate for the ith generic part

Π_Q = Quality factor for the ith generic part

N_i = Quantity of the ith generic part

n = Number of different generic part categories in the equipme

When deriving part failure rates from MIL-HDBK-217F, the following general assumptions are made.

- Use Environment – The environmental stresses applicable to the 7300 analog systems falls into the category of Ground Benign (G_B). Ground Benign environment is representative of a nonmobile, temperature and humidity controlled environment that is readily accessible to maintenance.

- Temperature – G_B environment is based on either a temperature of 50 °C for dynamic devices (microcircuits and discrete semiconductors) and 30 °C for static devices (resistors, capacitors, inductive devices, relays, switches, connectors, crystals, fuses, interconnection assemblies, connections, meters, lamps, filters or other miscellaneous parts). G_B temperatures are representative of the environment that the equipment is expected to function in during normal operation. Where vendor

data on a specific component is rated for temperatures greater than G_B, the base failure rate associated with this component is derated to agree with the G_B environment.

- Quality Factor – Typically a non-military or commercial grade quality factor is assigned. This is generally the most conservative category.

7.5.1.2 Application of the Methodology

The following steps are taken to provide sufficient data for the comparison between the ASIC-Based NXX Main Board and Personality Modules to the 7300 analog cards styles using the methodology stated above. For ease of the calculations, a "building block" approach was used. This building block approach takes into account all components that are "active" during normal operation. No "active" components are excluded by the use of this approach. The following building blocks were evaluated.

- Analog Input Type 1 (clock circuit included)
- Analog Input Types 2, 3 & 4
- Analog Output (with 4-20 mA current loop output/1-5 V voltage loop output)
- Analog Output (without current or voltage loop outputs)
- Operator Interface
- ASIC Interface (with diagnostics)
- Clock Divider, DAC Interface, 5x40 SRAM, Trouble and General Alarms & Combinational Logic
- Power Supply Modules
  - +5 VDIG
  - +/-5 VANALG & +/-15 V
  - +15 VISO & +5 VISO/+2.5 VISO
  - +5V/+2.5V
  - FP +60/+45/+30/+15
  - +24/+26 VIN
- Board & Connectors for Digital I/O boards (NAC, NAL, NCD, NCB, NTD)
- Board & Connectors for Isolated Voltage/Current Outputs boards (NSCG04, NLPG02, NLPG03)
- Board & Connectors for NCH, NLL, NLPG01, NLPG04, NLPG05, NMA, NMD, NRA, NSA, NSCG01, NSCG02, NSCG03, NSCG05, NSCG06, NSCG07, NSCG08, NVP

The method used for the parts count MTBF assessment is as follows.

(1) Failure rate calculations are performed for each of the building blocks on the ASIC-Based NXX Main Board.

(2) Failure rate calculations are performed for each of the Personality Modules (14 total).

(3) Using the following design input, operability determinations are made to judge which components within a building block on the NXX Main Board are active during normal operation. Components that are inactive during normal operation are not included in the MTBF calculations.

- Components associated with calibration mode are not included in the MTBF calculations.
- Only the Dual Port RAM on the Operator Interface is active during normal operation. All other components associated with the Operator Interface are associated with calibration mode and are therefore excluded from the MTBF calculations.
- The EPROMs that configure the Operator Interface and RAM Logic FPGAs on the NXX Main Board are not included in the MTBF calculations because these components are only used during power-up and then become inactive.
- All components associated with the diagnostic circuits are included in the MTBF calculations

(4) Failure rate calculations are recalculated for the building blocks using only the active components.

(5) Personality Module Input/Output/Power Supply Requirements are based on the equivalent 7300 analog card style.

(6) Failure rate calculations are performed for the NXX Main Board and the Personality Modules (14 total) using the individual Personality Modules NXX Main Board Input/Output/Power Supply requirements. Components associated with the power supply modules not required to support operation of a Personality Module are not included as they are considered to be inactive for that Personality Module to perform its intended function.

(7) Failure rate calculations are performed for each of the 7300 System analog card styles and groups targeted for replacement [54 total].

(8) Comparisons are made between the ABRM NXX Main Board/Personality Modules and the 7300 System analog cards targeted for replacement.

(9) Comparisons are made between the ABRM NXX Main Board/Personality Modules and the NXX Design Specification (Reference 7.7.3) reliability prediction of 100,000 hours MTBF at 30°C per function.

7.5.2 Functional Block Analysis (FBA)/Failure Modes & Effects Analysis (FMEA)

7.5.2.1 Methodology

For the ABRM Modes and Effects Analysis (FMEA), the traditional FMEA methodology described in MIL-STD-1629A and the Functional Block Assessment (FBA) methodology are used with the same operability determinations as those used for the parts count MTBF calculation. Card-level FMEAs are assembled based on the results of the building block FMEAs and FBAs in order to support the comparisons with the 7300 System analog card configurations being replaced. The failure effects are identified to the card-level, since this information is most useful in providing a comparison with the 7300 analog cards being replaced.

The FMEA methodology concentrates on identifying the effects of all credible single failures of components or subcomponents within a system. In a traditional FMEA application, the analysis focuses on failures of hardware elements within a system. The sub-component, credible failure mode, local and/or system level effects, and detection methods are identified in a qualitative FMEA. Optionally, quantitative FMEA techniques identify the rate or probability at which a given failure mode can occur. The traditional FMEA approach, however, becomes unpractical when analyzing complex digital technologies (i.e., the ASIC chip and FPGAs). For these types of devices, the FBA methodology is used.

Traditionally the FBA method has been used by Westinghouse as a tool for analyzing the failure modes and effects of complex systems in support of system licensing. The FBA is similar to the traditional FMEA method in that possible failure modes and system effects are analyzed. However, the FBA is focused on the functions necessary for the system to perform its intended function, rather than on the specific hardware components that make up that function.

Recognizing that the ASIC can be configured in a number of ways, the FBA covers all of the basic functions performed by the ASIC for all configurations of the 7300 System analog cards. This approach minimizes the effort in providing multiple ASIC module configuration assessments. It is important to note that in application, the FBA method evaluates the same hardware as the FMEA. Specifically, the FBA addresses groups of hardware as functional units and applies specific failure analysis at the equivalent functional level; whereas, the FMEA evaluates the hardware at the component level and assigns failure modes based upon an individual component failure and effect.

7.5.2.2 Application of the Methodology

The following steps are taken to provide sufficient data for the comparison between the ASIC-Based NXX Main Board and Personality Modules to the 7300 System analog cards targeted for replacement using the methodology described above. The FMEA/FBA Tables provided in Reference 7.7.23 are based on the following assumptions:

- The Controller code does not impact the reliability assessment because: 1) the Controller code contains no branches, loops, undefined states, makes any decisions on data or cannot lockup resulting in a fail-as-is condition; and 2) fail-as-is can only be the result of a hardware failure.

- No transient failures are considered; i.e., only persistent hardware failures are assessed.

- Failures to properly configure the ASIC-Based Main Board and Personality Modules(s) are considered to be an operational (human factors) type error, not a system failure.

The method used for the FMEA/FBA assessment is summarized as follows.

(1) A building block FMEA is performed on each Personality Module (14 total). The failure mode, detection method and effects are identified.

(2) A building block FMEA/FBA is performed on the ASIC-Based NXX Main Board. The component, failure mode, detection method and effects are identified.

(3) Card level failure mode assessments are performed using the information provided in the building block ASIC-Based NXX Main Board FBA and Personality Module FMEAs.

(4) A credible failure mode assessment for the 7300 System analog cards is performed to determine the failure modes associated with the existing analog cards. No component level FMEA/FBAs on the 7300 analog cards were performed as part of this assessment. Using the credible failure mode assessment for the 7300 System analog cards, the failure modes predicted for the ASIC-Based NXX Main Board and Personality Module(s) are compared to the equivalent analog system card to determine if any new failures are created as a result of the ASIC-Based replacement card designs.

7.5.3 7300 Analog Credible Failure Mode Assessment

7.5.3.1 Methodology

To determine if any new failure modes are created as a result of the ABRM Program, a credible failure mode assessment of the 7300 System analog card styles targeted for replacement by the ASIC-Based NXX Main Board and Personality Modules was performed. No component level FMEA/FBAs on the 7300 analog cards were performed as part of this assessment.

The following approach was used for this assessment. Each of the 7300 System analog card styles was divided into the postage stamps associated with a given card type based on the associated schematic. The credible failures of each postage stamp (not each component) were

then determined along with the detection method for each of the credible failures on the individual card outputs.

7.5.3.2 Application of the Methodology

The following steps are taken to identify the credible failures associated with the 7300 System analog cards using the methodology and assumptions provided above.

(1) For each of the 7300 analog card styles, the postage stamps for all groups associated with a style are identified.

(2) Each postage stamp is examined to determine the function, input/output requirements and power requirements. Critical components are identified in a postage stamp where applicable.

(3) For each postage stamp, the credible failure modes are identified.

(4) The failure modes for each postage stamp are collectively reviewed to determine the card level credible failure mode.

(5) Detection methods are identified for each failure type.

The data provided from this assessment were used to determine if any new failure modes are created with the application of the ASIC-Based replacement modules.

7.6 RESULTS SUMMARY

7.6.1 Parts Count MTBF Calculations

Using the methodology and the assumptions provided above, the results for the MIL-HDBK-217F parts count assessment are summarized below. A parts count assessment for each of the 7300 System analog card style(s)/groups was also performed to allow a comparison of the 7300 analog card styles/groups calculated MTBFs to the ASIC-Based NXX Main Board and Personality Module(s). The parts count also supported a comparison of the calculated MTBFs for the ASIC-Based NXX Main Board and Personality Module(s) to the reliability specification provided in Reference 7.7.3. The results of the detailed assessment is provided in Reference 7.7.23.

The following is a summary of these calculations.

- The calculated MTBF for all fourteen of the ASIC-Based NXX Main Board and Personality Modules exceeded the calculated MTBF for the equivalent 7300 analog card styles. Of these fourteen card styles, 10 of these card styles doubled the calculated MTBF for the equivalent 7300 analog card styles.

- All fourteen of the ASIC-Based NXX Main Board and Personality Modules exceed the design specification value of 100,000 hours at 30 °C at the functional level.

7.6.2 Functional Block Analysis/Failure Modes & Effects Analysis

A summary of the detailed FMEA for the ASIC-Based Replacement Modules (Reference 7.7.23) is provided below. For discussion purposes, the card styles have been grouped into the following categories.

- Comparators: NAC and NAL
- Controllers: NCB, NCD and NTD
- Analog Signal Processors: NCH, NLL, NMA, NMD, NRA, NSA and NSC
- Isolator and Loop Power Supply: NLP
- Voltage to Pulse Converter: NVP

Per the Input/Output/Power Supply requirements for the equivalent 7300 card styles, the following conclusions may be made. All failure modes that affect the ABRM function are detectable by surveillance testing, as they are for the 7300 System analog card. Periodic verification of channel measurements, via Channel Check surveillances, will validate both the existence of process noise and proper signal functioning. Additionally, many failures, (e.g., power failures, ASIC/control failures, and logic failures) are immediately detectable via the General Alarm. For those failures not immediately detectable, it is the intent that the periodic surveillance program, e.g., calibrations and functional testing, performed at Technical Specification intervals, will detect these types of failures and result in the proper corrective action being applied.

For the card styles with digital outputs (NAC, NAL, NCD, NTD), all failures will result in either failure to the logic true or failure to the logic false states, although the actual state of the signal depends upon the style of digital output implemented for the given card configuration (e.g., current sinking vs. current blocking). All of these failure modes are present with the existing 7300 System.

For the card styles with analog outputs (NCB, NCD, NTD, NCH, NLL, NMA, NMD, NRA, NSA, NSC, and NLP), all failures result in one of the analog output failure modes of fail high, fail low, signal drift, or fail-as-is, which are the same as the existing 7300 System. For inputs to high, median or low select functions, the fail-as-is failure mode will result in that function either being selected or not being selected, but it will be conservative with respect to the intended safety function. In the event of this condition, redundant channels are available to provide the protection to the plant safety limits in the presence of a single failure.

For the controller cards (NCB, NCD and NTD), the fail-as-is failure mode represents approximately less than four percent of the total failure rate for each card configuration. For the

analog signal processing cards (NCH, NLL, NMA, NMD, NRA, NSA and NSC), the fail-as-is failure mode represents approximately less than six percent of the total card failure rate. For the isolator and loop power supply card (NLP), the fail-as-is failure mode represents approximately less than four percent of the NLP card failure rate.

For the voltage to pulse converter card (NVP), the potential failure modes are pulse frequency fails high, fails low, frequency drift, or fail-as-is. The fail-as-is failure mode represents less than one percent of the total card failure rate. Also, since the pulse train output feeds control functions such as batch controllers, this failure will be detected due to the affect on the control function (increase in response to demand).

Although the relative significance of the various failure modes changes somewhat with the ASIC-Based module design, the overall module failure rate is less than the equivalent 7300 analog module.

7.6.3 7300 Analog Credible Failure MODE Assessment

Using the methodology and assumptions provided above, the credible failure modes for the postage stamps on the 7300 analog card styles are summarized as follows.

- Current Sinking (loss of signal/saturated signal)
- Current Blocking (loss of signal/saturated signal)
- Fail High Sinking (loss of signal/saturated signal)
- Fail Low Sinking (loss of signal/saturated signal)
- Loss of Manual Control
- Loss of Signal (Fail Low)
- Saturated Signal (Fail High)
- Signal Drift
- Fail-As-Is

Most failure modes listed above are associated with the output driver stage of a card style. Input failures may result in a Loss of Signal, Saturated Signal, Loss of Manual Control, Signal Drift or Fail-As-Is condition. Most failures (with the exception of those resulting in loss of manual control, Signal Drift or Fail-As-Is) will be immediately detectable via periodic Channel Checks (via the monitoring of process noise on redundant indications) and other Surveillance Tests (which will detect and correct signal drift or a fail-as-is condition). Loss of manual control will be immediately detectable only when manual control is demanded or by Surveillance Test alone. The results of the detailed assessment is provided in Reference 7.7.23.

7.7 REFERENCES

7.7.1 MIL-HDBK-217F, with Notice 1 and Notice 2, "Military Handbook Reliability Prediction of Electronic Equipment," February 28, 1995.

7.7.2 Reliability Analysis Center, FMD-91, "Failure Mode/Mechanism Distributions," 1991.

7.7.3 W Design Specification 413A63, "NXX Design Specification," 2/11/97, Rev. 0.

7.7.4 W Design Specification 413A66, "ASIC Design Specification," 11/19/96, Rev. 0.

7.7.5 W Design Specification 413A67, "ASIC Interface Specification," 11/19/96, Rev. 0.

7.7.6 W Design Specification 413A69, "ASIC Functional Description," 8/22/96, Rev. 0.

7.7.7 W Drawing 5D63629, "7300A ASIC-Based NXX Main Board Schematic," Rev. 0.

7.7.8 W Drawing 59B1002, "7300A ASIC-Based Personality Module NAC Analog Comparator Schematic Diagram," Rev. 0.

7.7.9 W Drawing 59B1003, "7300A ASIC-Based Personality Module NAL Signal Comparator Schematic Diagram," Rev. 0.

7.7.10 W Drawing 59B1004, "7300A ASIC-Based Personality Module NCB Controller Schematic Diagram," Rev. 0.

7.7.11 W Drawing 59B1005, "7300A ASIC-Based Personality Module NCD Controller Driver Schematic Diagram," Rev. 0.

7.7.12 W Drawing 59B1006, "7300A ASIC-Based Personality Module NCH Function Generator Schematic Diagram," Rev. 0.

7.7.13 W Drawing 59B1007, "7300A ASIC-Based Personality Module NLL Lead/Lag Schematic Diagram," Rev. 0.

7.7.14 W Drawing 59B1008, "7300A ASIC-Based Personality Module NLP Isolator and Loop Power Supply Card Schematic Diagram," Rev. 0.

7.7.15 W Drawing 59B1009, "7300A ASIC-Based Personality Module NMA Analog Mixing Amplifier Card Schematic Diagram," Rev. 0.

7.7.16 W Drawing 59B1010, "7300A ASIC-Based Personality Module NMD Multiplier/Divider Schematic Diagram," Rev. 0.

7.7.17 W Drawing 59B1011, "7300A ASIC-Based Personality Module NRA RTD Amplifier Card Schematic Diagram," Rev. 0.

7.7.18 W Drawing 59B1012, "7300A ASIC-Based Personality Module NSA Summing Amplifier and Median Select Schematic Diagram," Rev. 0.

7.7.19 W Drawing 59B1013, "7300A ASIC-Based Personality Module NSC Signal Converter Schematic Diagram," Rev. 0.

7.7.20 W Drawing 59B1014, "7300A ASIC-Based Personality Module NTD Tracking Driver Schematic Diagram," Rev. 0.

7.7.21 W Drawing 59B1015, "7300A ASIC-Based Personality Module NVP Voltage-to-Pulse Converter Schematic Diagram," Rev. 0.

7.7.22 W Calc Note RE-433, Rev. 1 "ASICs vs. 7300 Analog Parts Count MTBF Reliability Assessment"

7.7.23 W WCAP-14975 "7300A ASIC-Based Replacement Module Reliability Assessment and Failure Modes and Effects Analysis," September 1997, Rev. 0

8.0 WESTINGHOUSE SAFETY EVALUAION

This section provides a standard approach for preparation of a plant specific 10 CFR 50.59 safety evaluation to facilitate installation of ABRM modules in place of 7300 system analog modules. Sufficient information is provided to conclude that implementation of the ABRM card in protection and control system applications does not result in an unreviewed safety question.

8.1 LICENSING APPROACH

The licensing approach for implementation of an ABRM module replacement under 10 CFR 50.59 includes a design that is equivalent in form, fit, and function and that contains no software (programmable code, special procedures) in any aspect of the replacement modules. Reference 8.4.1 is a Failure Modes and Effects Analysis (FMEA) which demonstrates that the replacement card introduces no new failure modes at the system level other than those considered previously for analog systems. A utility subgroup continuously evaluated the design to assure that no unreviewed safety question exists. The NRC's attendance and participation in periodic meetings assured their input and review during the development process. The ABRM Licensing Summary Report, Reference 8.4.6, describes the development process with a thorough description of testing and functional equivalency. The report was submitted to the NRC for approval. Any utility intending to replace their 7300 System analog boards with ASIC-Based boards should reference the Licensing Summary Report and address any conditions stated in the associated NRC Safety Evaluation in their plant specific safety evaluation.

8.2 SAFETY EVALUATION

A functionally equivalent card has been developed to replace 7300 Process Protection System (PPS) and Process Control System (PCS) analog cards. This replacement card is the same size as the existing analog 7300 System printed circuit board, and it contains an ASIC chip that replaces most of the discrete components mounted on the analog board.

8.2.1 Background

The replacement card utilizes an ASIC chip to develop process functions digitally. The ASIC chip consists of dedicated functional math segments that can only result in the performance of the intended process function as selected by a passive header through a controller. The controller, which is a loop of instructions with no branches, acts as an on/off sequencer for the segments (simple math functions) on the ASIC chip.

On the ASIC chip, circuits are hard-wired to form the math functions. Independent simulation testing, followed by actual device tests, demonstrated that all circuits are operational. Incorrect results can only occur through a random hardware failure. No undefined states can exist since each cycle is predetermined and will go to completion (with no decisions or branching) as long as there is no momentary interruption (e.g., power loss, clock failure). The sequence starts over after a power interruption. The system cannot be overloaded or "hang-up". For example, if a division by zero occurs in one cycle, all ones appear for that cycle or as many cycles as the

denominator remains zero. Once the denominator becomes non-zero, the calculation will be correct.

The FMEA, Reference 8.4.1, on the replacement card demonstrates that although no new failure modes exist, utilizing ASIC-Based technology would result in the card being more susceptible to a fail-as-is condition than a completely analog card. This condition is detectable by periodic surveillance and will normally result in a card General Alarm. Reference 8.4.1 also contains a reliability analysis that demonstrates an improvement in reliability over the existing analog cards. Each card is subjected to a dedication process, which includes functional tests to assure operability. Environmental testing, Reference 8.4.2, Seismic testing, Reference 8.4.3, EMC, Electrical Fast Transient and Surge testing, Reference 8.4.4, and Fault testing, Reference 8.4.5, complete the ABRM qualification and dedication process.

8.2.2 Determination of Unreviewed Safety Question

1) May the proposed activity increase the probability of occurrence of an accident evaluated previously in the Safety Analysis Report (SAR)?

   The FMEA, Reference 8.4.1, demonstrates that the replacement card using ASIC-Based technology introduces no new failure modes at the system level and therefore no new effects or consequences other than what has been considered previously for analog systems. The technology introduces no new performance characteristics that increase the need for operator intervention during any plant condition. The design includes features that minimize control system action following a failure on a control system card. Per References 8.4.2 through 8.4.5, the component, card, or system has been demonstrated to be compatible with existing environments (e.g., temperature, humidity, seismic, EMI/RFI). Utilizing ASIC-Based technology for 7300 System replacement modules will not increase the probability of occurrence of an accident.

2) May the proposed activity increase the consequences of an accident evaluated previously in the SAR?

   The architecture of an ASIC-Based module and/or system (mixed with analog cards or all ABRM modules) maintains the functional independence by channel that exists in the analog system (i.e., no central processor). The human-machine interface does not involve operator actions credited in the licensing basis. Common cause software failures are not a concern with the non-software based ASIC technology which does not introduce any new failure modes at the system level and therefore no new consequences other than those considered previously in the analog system. Per Reference [insert plant specific analysis here], the accuracy and response time of the ABRM or system has been demonstrated to be within acceptable criteria to conform with the safety analysis, so that utilizing ASIC-Based technology will not increase the consequences of an accident.

3) May the proposed activity increase the probability of occurrence of a malfunction of equipment important to safety evaluated previously in the SAR?

Per References 8.4.2 through 8.4.5, the replacement card has been demonstrated to be compatible with existing environments (e.g., temperature, humidity, seismic, and EMI/RFI). Engineering tests have been performed to assure compatibility with existing analog cards. The ASIC-Based technology reduces the internal cabinet thermal loads below that of the analog only systems; therefore, the existing cabinet cooling and plant HVAC is adequate. The ASIC chip's hard-wired technology is a direct form, fit, and functional replacement for the analog system, maintaining separation and independence. An incorrect result can only occur through a hardware failure. These hardware failures are similar to those of the current analog system in that they do not result in a common mode failure, as might be a concern with a software-based card. Therefore only one of the four redundant protection channels will fail at one time, consistent with the current licensing basis. The increase in reliability demonstrates that a hardware malfunction is less likely than that which could occur with the present analog cards. Therefore, the application of ASIC-Based technology will not increase the probability of occurrence of a malfunction of equipment important to safety.

4) May the proposed activity increase the consequences of a malfunction of equipment important to safety evaluated previously in the SAR?

The FMEA, Reference 8.4.1, demonstrates that the replacement card based on ASICs technology, which does not rely on software, does not introduce any new failure modes at the system level and therefore no new consequences other than those considered previously in the analog system. The card does not have a default state upon loss of power and will restore to the operating parameters and settings when power is returned. The design of the system ensures that any human-machine interface will not introduce failure modes different from those in the existing analog system. Therefore, the consequences of a malfunction of equipment important to safety have not been increased.

5) May the proposed activity create the possibility of an accident of a different type than any evaluated previously in the SAR?

The FMEA, Reference 8.4.1, shows that ASIC-Based technology introduces no new failure modes at the system level and therefore no new effects or consequences other than what has been considered previously for analog systems. The ASIC-Based card is designed to be compatible with the specifications of existing power supplies and cards. The systems are designed and qualified so that common mode failures in these accident mitigation systems are not a concern, and replacement with ASIC-Based technology does not create the possibility of an accident not previously evaluated.

6) May the proposed activity create the possibility of a malfunction of equipment important to safety when the malfunction is of a different type than any evaluated previously in the SAR?

The FMEA, Reference 8.4.1, shows that ASIC-Based technology introduces no new failure modes at the system level and therefore no new effects or consequences other

than what has been considered previously for analog systems. On a card level, the ASIC-Based technology may be more susceptible to a fail-as-is mode than an analog card. Since the technology is not software based, there is no potential common cause. Therefore, this condition would only be the result of a single hardware failure and is easily detectable during periodic channel checks, functional testing and/or calibration. Per References 8.4.2 through 8.4.5, the ASIC-Based card has been demonstrated to be compatible with existing environments (e.g., temperature, humidity, seismic, and EMI/RFI) and will not create an environment that would impact other plant instrumentation or equipment. The FMEA, Reference 8.4.1, demonstrates that the application of ASIC-Based technology via the replacement card does not create the possibility of malfunction not previously evaluated.

7) Does the proposed activity reduce the margin of safety as defined in the basis for any technical specification?

Per Reference [insert plant specific analysis here] the accuracy and response time of an ASIC-Based card or system has been demonstrated to be at least equivalent to the existing analog system which conforms with the safety analysis and the supporting setpoint uncertainty calculations, so that utilizing ASIC-Based technology will not reduce the margin of safety as defined in the basis for any technical specification.

8.3 CONCLUSION

Design features that support licensing under 10 CFR 50.59 include the implementation of simple, dedicated mathematical functions that consist of logic circuits hardwired to perform the intended function. The simplicity of the design facilitates verification and validation through a combination of test bus and test vectors. The testing enables a thorough fault coverage, demonstrating that no latent failures exist and that all circuits are working. Actual test results were compared to independent simulation test results. The operation of the card is deterministic with each cycle being completed with no decisions made on data and no branches, loops or undefined states. Before the card is put into service, the function is selected and confirmed by test.

Installation of the ASIC-Based replacement cards in the PPS and PCS will maintain the reliability and performance of the system. The evaluation has addressed EPRI TR-102348, "Guideline on Licensing Digital Upgrades". The performance and qualification of the card have been demonstrated, and the ABRM module does not introduce any new failure modes other than those considered previously for the analog system. Since the card is still analog-in/analog-out, there is no change required to the testing definitions of the Technical Specifications. Therefore, installation of the ASIC-Based replacement cards does not constitute an unreviewed safety question as defined by 10 CFR 50.59 (a)(2).

8.4 REFERENCES

8.4.1 Westinghouse WCAP-14975, Revision 0, "7300A ASIC-Based Replacement Module Reliability Assessment and Failure Modes and Effects Analysis," September, 1997.

8.4.2 Westinghouse WCAP-15378, Revision 0, "Environmental Test Report for Westinghouse ASIC-Based Replacement Module for 7300 Process Protection System," February 2000.

8.4.3 Westinghouse WCAP-15215, Revision 0, "Seismic Test Report for Westinghouse ASIC-Based Replacement Module for 7300 Process Protection System," May 1999.

8.4.4 Westinghouse WCAP-15403, Revision 0, "EMC Test Report for Westinghouse ASIC-Based Replacement Module for 7300 Process Protection System," April 2000.

8.4.5 Westinghouse WCAP-15371, Revision 0, "Fault Conditions Test Report for Westinghouse ASIC-Based Replacement Module for 7300 Process Protection System," February 2000.

8.4.6 Westinghouse WCAP-15413, Revision 0, "Westinghouse 7300A ASIC-Based Replacement Module Licensing Summary Report," May, 2000.

9.0 SUPPLEMENTAL REPORT ON RESPONSE TIME TEST DELETION

Reference 9.6.1 is the report approved by the NRC that justifies elimination of periodic response time testing of selected RTS and ESFAS equipment, based on Failure Modes and Effects Analysis (FMEA). To provide verification of the analysis conclusions and to establish certain bounding response times, the FMEA was supplemented by actual testing of selected equipment, including simulation of degraded components, where appropriate. The objective of this section of the ABRM Licensing Summary Report is to show that relaxing the requirements to perform periodic response time testing (RTT) on the 7300 Process Protection System ABRM replacement modules is justified.

Since testing of the 7300 rack electronic circuit boards determined that marginal component degradation could affect response time and may not be detectable during routine calibration tests, the justification for eliminating the RTT is based on bounding circuit response times. Bounding circuit response times were established by analyzing circuits with exaggerated component degradations. The FMEA demonstrated that response time limits can be bounded and that periodic verification testing is not needed to ensure that response time limits assumed in the safety analysis are preserved.

Reference 9.6.1 applied FMEA and the results of tests to the electronic signal processing portion of the protection system circuitry to justify relaxation of periodic response time testing of this portion the channel. Included in this program was the Westinghouse 7300 System of analog process protection equipment. Since the ABRM module is a direct replacement for the 7300 System analog cards included in the program, it is desirable to maintain elimination of response time testing when an analog card is replaced with the equivalent ABRM.

The ABRM Main Board/Personality Modules that are common to the 7300 analog boards analyzed in Reference 9.6.1 are:

NLP Loop Power Supply and Isolator;

NSA Summing Amplifier;

NAL Analog Comparator;

NCH Function Generator;

NMD Multiplier/Divider; and

NRA RTD Amplifier.

The same methodology used in Reference 9.6.1 was used to analyze the ABRMs. The FMEA circuit analysis determined which components on the Main Board and Personality Modules were critical to response time. In lieu of testing, due to the less complex ABRM, the analysis

took into account catastrophic component failure and degraded component performance to determine a bounding response time for the ABRM modules. This response time bounds the limit to which response time can be increased by degraded or failed components without that degradation or failure affecting calibration. The FMEA shows that component degradation will not increase the response time beyond the bounding response time without that degradation being detectable by other periodic surveillance tests, such as channel checks, functional tests and/or calibrations.

9.1 METHODOLOGY

The justification for the elimination of periodic response time testing is based on the Failure Modes and Effects Analysis that either determined that individual component degradation had no response time impact, or identified components that may contribute to trip system response time degradation. Where potential response time impact was identified, analysis was performed to determine the magnitude of the response time degradation and a bounding response time limit for the component was determined. The bounding response time allocation is derived from design response time specification for the module. For the ABRM Main Board and Personality Modules, the FMEA was performed by having a circuit designer review the circuits and identify those components that may increase response time if they degrade from their nominal value. The FMEA does the following:

- Identifies response time sensitive components on the Main Board and Personality Modules via circuit analysis;
- Evaluates impact on response time if a component fails or degrades;
- Identifies detectability of degraded components via calibration; and
- Identifies components that impact calibration but not response time.

The analysis identified capacitors and resistors as the dominant response time sensitive components. Increased resistance and capacitance tend to increase response time. Based on the information contained in Reference 9.6.1, a conservative increase of 50% in capacitance was used to determine the maximum change in response time for capacitor degradation. Resistors were assumed to degrade as much as 200% of the nominal resistance, which is a conservative increase based on engineering judgement.

An input step change was used to analyze response time. Response time is defined as the time to reach 63% of the final output. This time is equal to the time constant of a dynamic system with a characteristic first order lag. A slightly more conservative limit of 67% was used for direct comparison to the analog card response times reported in Reference 9.6.1.

9.2 PROGRAM RESULTS

The evaluation for the ABRM modules consisted of a FMEA on the following cards that are in the path of a trip or actuation signal:

NXX ABRM Main Board;

NAL Comparator Personality Module;

NCH Function Generator Personality Module;

NLL Lead/Lag Personality Module;

NLP Loop Power Supply and Isolator Personality Module;

NMD Multiplier/Divider Personality Module;

NRA RTD Amplifier Personality Module; and

NSA Summing Amplifier Personality Module.

The NXX Main Board was analyzed by itself. The Personality Modules were then analyzed, and the response time of the Personality Module was added to the response time of the Main Board. The cumulative response time is the combination of the Main Board with its respective Personality Module for each potential replacement application.

The FMEA provided the basis for determining that the ABRM modules do not require testing to quantify the effect of component degradation on the system response time. The potential increases in response time that cannot be detected by calibration are easily evaluated by assuming both a 200% increase in resistance plus a 50% increase in capacitance and are accounted for in the overall channel response time allocation for the ABRM modules. During validation testing, each module was tested to provide a baseline response time value. The nature of the ABRM modules is such that there is no wear out potential for the process algorithm performed in the ASIC chip. Any algorithm error, which may cause an unacceptable response time, is a design flaw, which would have been detected during validation testing. Since most of the process function is performed by the algorithm executed within the ASIC chip, the only components contributing to response time are the components in the input and output signal conditioning circuitry. This simplified the FMEA analysis and eliminated the need to verify bounding response times by testing with degraded component values.

9.2.1 NXX - ABRM Main Board

The response time of the Main Board is dominated by the ADC and its internal 10 Hz process noise digital filter. Using data supplied by the ADC vendor, the nominal response time of the ADC and internal digital filter was calculated to be 44.8 milliseconds. Algorithm execution time is either 1.024 or 2.048 milliseconds, depending on algorithm size. All other components add a nominal delay of 1.4 milliseconds, resulting in a nominal response time of 47.2 or 48.2 milliseconds for the Main Board. With a conservative maximum degradation factor of two for resistors and 1.5 for capacitors, the increase in response time was calculated to be 2.8 milliseconds, resulting in a bounding response time allocation for the Main Board of 50.0 or 51.0 milliseconds.

9.2.2 NAL - Comparator Personality Module

There are no components on the NAL Personality Module that add to the response time of the Main Board. The NAL algorithm execution time is 1.024 milliseconds. Therefore, the NAL ABRM bounding response time allocation is the same as the Main Board, 50.0 milliseconds.

9.2.3 NCH - Function Generator Personality Module

There are no components on the NCH Personality Module that add to the response time of the Main Board. The NCH algorithm execution time is 1.024 milliseconds. Therefore, the NCH ABRM bounding response time allocation is the same as the Main Board, 50.0 milliseconds.

9.2.4 NLL - Lead/Lag Personality Module

The time response of dynamic functions (i.e., lag, lead/lag and derivative) is verified during periodic calibration testing. However, the modules can be set-up to operate with proportional gain only (i.e., no dynamic function). The NLL ABRM was analyzed for these applications. There are no components on the NLL Personality Module that add to the response time of the Main Board. The NLL algorithm execution time is 2.048 milliseconds. Therefore, the NLL ABRM bounding response time allocation is 51.0 milliseconds.

9.2.5 NLP - Loop Power Supply and Isolator Personality Module

The NLP ABRM has isolated and non-isolated analog outputs. Only the non-isolated analog output supplies protection system functions. The nominal increase in response time due to the NLP Personality Module is 10 milliseconds. With the most sensitive response time capacitor degraded to 1.5 times the nominal value plus the resistor degraded to 2.0 times the nominal value, the maximum expected increase in response time for the NLP Personality Module is 20 milliseconds. If the same capacitor decreases in value, opens, or shorts, the response time of the module is faster, or the module fails, or the degradation is detectable by a calibration test. The NLP algorithm execution time is 1.024 milliseconds. Therefore, the NLP ABRM bounding response time allocation is 80.0 milliseconds. This allocation equals the bounding response time of the NXX Main Board (50.0 milliseconds) plus the bounding response time of the NLP Personality Module (30 milliseconds).

9.2.6 NMD - Multiplier/Divider Personality Module

There are no components on the NMD Personality Module that add to the response time of the Main Board. The NMD algorithm execution time is 1.024 milliseconds. Therefore, the NMD ABRM bounding response time allocation is the same as the Main Board, 50.0 milliseconds.

9.2.7 NRA - RTD Amplifier Personality Module

The NRA Personality Module contains a low pass filter consisting of resistors R_5 and R_9, and capacitor C_1. The nominal response time of this filter is 25.7 milliseconds. With a conservative maximum degradation factor of 2.0 for both resistors and 1.5 for the capacitor, the increase in

response time was calculated to be 51.5 milliseconds. The NRA algorithm execution time is 1.024 milliseconds. Therefore, the NRA ABRM bounding response time allocation is 127.2 milliseconds. This allocation equals the bounding response time of the NXX Main Board (50.0 milliseconds) plus the bounding response time of the NRA Personality Module (77.2 milliseconds).

9.2.8 NSA - Summing Amplifier Personality Module

There are no components on the NSA Personality Module that add to the response time of the Main Board. The NSA algorithm execution time is 1.024 milliseconds. However, the NSA algorithm contains a low pass filter that adds approximately 50.8 milliseconds to the delay time. Therefore, the NSA ABRM bounding response time allocation is 100.8 milliseconds. This allocation equals the bounding response time of the NXX Main Board (50.0 milliseconds) plus the response time of the NSA algorithm (50.8 milliseconds).

9.3 SUMMARY OF FMEA AND TESTING

The FMEA of the ABRM modules identified components on each module that impact response time if they degrade and the degradation will not be detectable by calibration or functional testing. The maximum response time change due to undetectable component degradation of the most sensitive components was determined by calculation for each module, and can be used as the bounding condition when considered in response time verification of the module or protection channel that uses the module. Each module was also tested for comparison against the nominal calculated value.

Table 9-1 provides the bounding response time allocations to be used when implementing the response time verification methodology described in Reference 9.6.1. Data from the calculated and tested nominal response times and the equivalent 7300 System analog card bounding response time contained in Reference 9.6.1 are also shown in the table.

TABLE 9-1

ABRM RESULTS/ANALOG COMPARISON

(All values in milliseconds)

ABRM	ABRM Nominal Response Time (calculated)	ABRM Actual Response Time (measured)	ABRM Bounding Response Time (calculated)	Equivalent Analog Module Bounding Response Time
NAL	47.2	50	50.0	5
NCH	47.2	50	50.0	67.5
NLL	48.2	50	51.0	NA
NLP	57.2	60	80.0	60
NMD	47.2	48.75	50.0	104
NRA	72.9	70	127.2	213
NSA	98.0	100	100.8	37.5

The data in Table 9-1 indicates the following:

(1) The difference between the nominal and bounding response times are:

- 2.8 milliseconds for NAL, NCH, NLL, NMD and NSA;
- 22.8 milliseconds for NLP; and
- 54.3 milliseconds for NRA.

(2) The accuracy of the actual response time measurements is approximately ± 5 milliseconds, due to test equipment accuracy and strip chart resolution. This, in conjunction with a difference of only 2.8 milliseconds between nominal and bounding response times, makes the actual response time values of the NAL, NCH, NLL, NMD and NSA appear to be the same as the bounding values.

(3) For the NLP, the actual response time (60 milliseconds) is within the test and measurement accuracy of the nominal calculated value of 57.2 milliseconds.

(4) For the NRA, the actual response time (70 milliseconds) is within the test and measurement accuracy of the nominal calculated value of 72.9 milliseconds.

(5) For the Personality Modules that do not contribute to the response time of the Main Board, the measured response time of the Main Board/Personality Module combination is consistent with the calculated value.

9.4 ABRM INSTALLATION

A plant that has incorporated elimination of periodic response time testing in accordance with Reference 9.6.1 must analyze the impact on response time of installing an ABRM module in place of the equivalent 7300 System analog card. However, the plant will not have to perform a new protection system baseline response time test when an ABRM module is used as a replacement for the equivalent 7300 System analog card because the nominal response time of the ABRM module is dominated by the ADC and its internal 10 Hz digital filter. The digital filter corner frequency (10Hz) is controlled by the master clock frequency (4 MHz). The master clock frequency is determined by the crystal. A small degradation in the crystal frequency will cause the oscillator to stop. If the oscillator stops, the card will not operate. Therefore, the installation of the ABRM modules does not require a new RTS/ESFAS baseline response time test.

9.5 CONCLUSION

Based on the results of Failure Modes and Effects Analysis with degraded components, justification is established for relaxing the periodic response time test of process protection channels using ABRM modules as direct replacements for the Westinghouse 7300 Process Protection System analog cards. In place of periodic tests, generic bounding response times were developed for ABRM modules for use in the determination of total response time for the RTS and ESFAS functions as required by Technical Specifications. Bounding response time allocations at the ABRM module level are provided so the plant staff can verify the specific response time for each protection system function based on the plant as-built configuration. Installation of the ABRM modules does not require a new RTS/ESFAS baseline response time test.

9.6 REFERENCES

9.6.1 Westinghouse WCAP-14036-P-A, Revision 1, "Elimination of Periodic Protection Channel Response Time Tests," October, 1998.

10.0 REGULATORY CRITERIA COMPLIANCE

10.1 COMPLIANCE WITH NRC GENERAL DESIGN CRITERIA (GDC)

Many of the GDCs listed in 10 CFR 50 Appendix A apply to the protection system design and do not impact the replacement of a 7300 analog card with an ABRM. Those criteria that have a potential impact are discussed.

GDC 1 - Quality Standards and Records

"Structures, systems, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. Where generally recognized codes and standards are used, they shall be identified and evaluated to determine their applicability, adequacy, and sufficiency and shall be supplemented or modified as necessary to assure a quality product in keeping with the required safety function. A quality assurance program shall be established and implemented in order to provide adequate assurance that these structures, systems, and components will satisfactorily perform their safety functions. Appropriate records of the design, fabrication, erection, and testing of structures, systems, and components important to safety shall be maintained by or under the control of the nuclear power unit licensee throughout the life of the unit."

Compliance: The introduction of the ABRM into the plant Process Protection System is accomplished through the same quality assurance programs that are in place at the utility for the present 7300 System. These programs, along with similar programs at the ABRM manufacturer and supplier ensure that the replacement modules are dedicated to perform the intended safety functions. A commercial dedication process was followed for fabrication of the actual ASIC chip. The commercial dedication is based on the fact that the design of the ASIC is simple, the chip and functions are thoroughly testable, and the ABRM Qualification and Validation Test Programs demonstrated that the chip performs as intended in a safety related function. The ASIC chip is mounted on the Main Board along with all other components that comprise the ABRM. The Main Board and Personality Modules were subjected to a series of tests. These tests consisted of EMC Performance and Environmental, Seismic, and Fault Qualification tests. The ABRM successfully passed all tests. The ABRM Validation Test Program (which included Abnormal Conditions and Events tests) demonstrated that the ASIC chip performed as intended for all module level process functions. Each module is commercially dedicated based on these type tests and factory tests developed to demonstrate the functional compliance of that particular module. Appropriate records are maintained throughout the installed life of the product.

GDC 2 - Design Bases for Protection Against Natural Phenomena

"Structures, systems, and components important to safety shall be designed to withstand the effects of natural phenomena such as earthquakes, tornadoes, hurricanes,

floods, tsunami, and seiches without loss of capability to perform their safety functions. The design bases for these structures, systems, and components shall reflect: (1) Appropriate consideration of the most severe of the natural phenomena that have been historically reported for the site and surrounding area, with sufficient margin for the limited accuracy, quantity, and period of time in which the historical data have been accumulated, (2) appropriate combinations of the effects of normal and accident conditions with the effects of the natural phenomena and (3) the importance of the safety functions to be performed."

Compliance: The existing 7300 Process Protection System has been qualified to withstand the effects of a seismic event without loss of the capability to perform the intended safety function. The ABRM has been successfully qualified to the same criteria as reported in WCAP-15215, "Seismic Test Report, Westinghouse ASIC-Based Replacement Module for the 7300 Process Protection System".

GDC 3 - Fire Protection

"Structures, systems, and components important to safety shall be designed and located to minimize, consistent with other safety requirements, the probability and effect of fires and explosions. Noncombustible and heat resistant materials shall be used wherever practical throughout the unit, particularly in locations such as the containment and control room. Fire detection and fighting systems of appropriate capacity and capability shall be provided and designed to minimize the adverse effects of fires on structures, systems, and components important to safety. Firefighting systems shall be designed to assure that their rupture or inadvertent operation does not significantly impair the safety capability of these structures, systems, and components."

Compliance: Introduction of the ABRM does not change the design of the plant with regard to minimizing the effects of fires and explosions. The modules are designed with similar fire resistant materials as the present 7300 System cards and are installed in a cabinet.

GDC 4 - Environmental and Missile Design Bases

"Structures, systems, and components important to safety shall be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents. These structures, systems, and components shall be appropriately protected against dynamic effects, including the effects of missiles, pipe whipping, and discharging fluids, that may result from equipment failures and from events and conditions outside the nuclear power unit. However, dynamic effects associated with postulated pipe ruptures in nuclear power units may be excluded from the design basis when analyses reviewed and approved by the Commission demonstrate that the probability of fluid system piping rupture is extremely low under conditions consistent with the design basis for the piping."

Compliance: The location of the 7300 Process Protection System precludes exposure to accident environments. The only environmental change that could impact the performance of the ABRM would be a temporary increase in temperature due to the loss of HVAC. The ABRM performance under these conditions has been successfully demonstrated as documented in WCAP-15378, "Environmental Test Report, Westinghouse ASIC-Based Replacement Module for the 7300 Process Protection System".

GDC 13 – Instrumentation and Control

"Instrumentation shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges."

Compliance: The ABRM has been designed and tested to replicate the functional capability of the existing 7300 Process Protection System. There has been no change in the functional requirements of the instrumentation and control system. Depending on the modules utilized in a given channel arrangement, the total response time may exceed that of the 7300 analog channel. Installing an ABRM will have no impact on the ability of the instrumentation and control system to assure plant safety and provide proper indication during all anticipated events as long as the response time is reviewed and accepted.

GDC 17 – Electric Power Systems

"An onsite electric power system and an offsite electric power system shall be provided to permit functioning of structures, systems, and components important to safety. The safety function for each system (assuming the other system is not functioning) shall be to provide sufficient capacity and capability to assure that (1) specified acceptable fuel design limits and design conditions of the reactor coolant pressure boundary are not exceeded as a result of anticipated operational occurrences and (2) the core is cooled and containment integrity and other vital functions are maintained in the event of postulated accidents . . . ."

Compliance: Installing the ABRM has no impact on the power supply since it consumes less power than the existing 7300 Process Protection System.

GDC 20 – Protection System Functions

"The protection system shall be designed (1) to initiate automatically the operation of appropriate systems including the reactivity control systems, to assure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational

occurrences and (2) to sense accident conditions and to initiate the operation of systems and components important to safety."

Compliance: The Process Protection System design has not changed. The installation of an ABRM does not impact the ability of the protection system to sense and respond to plant conditions by initiating appropriate action.

GDC 21 - Protection System Reliability and Testability

"The protection system shall be designed for high functional reliability and inservice testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection system shall be sufficient to assure that (1) no single failure results in loss of the protection function and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated. The protection system shall be designed to permit periodic testing of its functioning when the reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred."

Compliance: The protection system is designed for reliability and testability. As documented in WCAP-14975, "7300A ASIC-Based Replacement Module Reliability Assessment and Failure Modes and Effects Analysis", the calculated Mean Time Between Failure (MTBF) of the ABRM exceeds that of the equivalent 7300 analog card that it replaces. As with the analog cards, all failure modes that affect the ABRM are detectable by surveillance testing. The provisions for testability remain the same.

GDC 22 - Protection System Independence

"The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function."

Compliance: Installation of an ABRM does not change the redundancy and independence which are designed into the protection system. The ABRM utilizes high quality components, simplistic design, appropriate quality control and qualification along with existing surveillance capabilities to prevent the loss of the protection function.

GDC 23 - Protection System Failure Modes

"The protection system shall be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy (e.g., electric power, instrument air), or

postulated adverse environments (e.g., extreme heat or cold, fire, pressure, steam, water, and radiation) are experienced."

Compliance: The protection system is designed with consideration of the most probable failure mode, which in the case of either the 7300 analog or the ABRM is to initiate the protective action on loss of power. The ABRM is designed to replicate the 7300 analog system and a de-energize to trip mode can be implemented. No new failure modes were identified in WCAP-14975, "7300A ASIC-Based Replacement Module Reliability Assessment and Failure Modes and Effects Analysis".

GDC 24 – Separation of Protection and Control Systems

"The protection system shall be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired."

Compliance: By design, the protection and control systems are separate and distinct. In some cases, the control system input is derived from the protection system through an isolator. The ABRM isolators have been successfully tested to guard against a potential protection system impact by the application of a fault to the control side of the isolator. These fault tests are documented in WCAP-15371, "Fault Conditions Test Report, Westinghouse ASIC-Based Replacement Module for the 7300 Process Protection System".

GDC 25 – Protection System Requirements for Reactivity Control Malfunctions

"The protection system shall be designed to assure that specified acceptable fuel design limits are not exceeded for any single malfunction of the reactivity control systems, such as accidental withdrawal (not ejection or dropout) of control rods."

Compliance: Installation of an ABRM in the control system does not impact the single failure analysis of the reactivity control system since the FMEA (WCAP-14975, "7300A ASIC-Based Replacement Module Reliability Assessment and Failure Modes and Effects Analysis") concluded that the 7300 analog system and the ABRM have the same failure modes.

GDC 29 – Protection Against Operational Occurrences

"The protection and reactivity control systems shall be designed to assure an extremely high probability of accomplishing their safety functions in the event of anticipated operational occurrences."

Compliance: With the installation of an ABRM, the protection and reactivity control systems continue to have a high probability of performing their required safety functions. The system design and functionality has not changed and the quality assurance program remains the same. In addition, the ABRM MTBF, as documented in WCAP-14975, "7300A ASIC-Based Replacement Module Reliability Assessment and Failure Modes and Effects Analysis", exceeds that of the 7300 analog system cards it replaces.

10.2 COMPLIANCE WITH 10 CFR 50.55a(h)

"Protection systems. For nuclear power plants with construction permits issued after January 1, 1971, but before May 13, 1999, protection systems must meet the requirements stated in either IEEE Std. 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations," or in IEEE Std. 603-1991, "Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995. For nuclear power plants with construction permits issued before January 1, 1971, protection systems must be consistent with their licensing basis or may meet the requirements of IEEE Std. 603-1991 and the correction sheet dated January 30, 1995."

Most of the requirements in Section 4 of IEEE 279-1971 and section 5 of IEEE 603-1998 apply to the protection system design and do not impact the replacement of a 7300 analog card with an ABRM. Those requirements that have a potential impact are discussed by referring to the applicable paragraph in IEEE 279-1971.

Paragraph 4.3 Quality of Components and Modules

"Components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. Quality levels shall be achieved through the specification of requirements known to promote high quality, such as requirements for design, for the derating of components, for manufacturing, quality control, inspection, calibration and test."

Compliance: The introduction of the ABRM into the plant Process Protection System is accomplished through the same quality assurance programs that are in place at the utility for the present 7300 System. These programs, along with similar programs at the ABRM manufacturer/supplier ensure that the replacement modules are dedicated to perform the intended safety functions.

Paragraph 4.4 Equipment Qualification

"Type test data or reasonable engineering extrapolation based on test data shall be available to verify that protection system shall meet, on a continuing basis, the performance requirements determined to be necessary for achieving the system requirements."

Compliance: Seismic (WCAP-15215, "Seismic Test Report, Westinghouse ASIC-Based Replacement Module for the 7300 Process Protection System") and environmental (WCAP-15378, "Environmental Test Report, Westinghouse ASIC-Based Replacement Module for the 7300 Process Protection System") testing to the same levels as the 7300 analog system has been successfully completed on the ABRM.

Paragraph 4.7.2 Isolation Devices

"The transmission of signals from protection system equipment for control system use shall be through isolation devices which shall be classified as part of the protection system and shall meet all the requirements of this document. No credible failure at the output of an isolation device shall prevent the associated protection system channel from meeting the minimum performance requirements specified in the design bases."

Compliance: The ABRM protection/control isolation capability has been demonstrated as shown in WCAP-15371,"Fault Conditions Test Report, Westinghouse ASIC-Based Replacement Module for the 7300 Process Protection System". The isolation modules were designed, so that a short circuit, open circuit or the application of a credible fault on the output of the isolator will not affect the input (protective side) of the isolator.

Paragraph 4.18 Access to Setpoint Adjustments, Calibration and Test Points

"The design shall permit the administrative control of access to all setpoint adjustments, module calibration adjustments, and test points."

Compliance: The design of the ABRM provides access to setpoint adjustments and module calibration through the Operator Interface. Setpoints and tuning constants are entered through the Operator Interface which provides the ability to change these values by accessing memory locations. When the desired setting is obtained, the digital value representing the analog voltage is locked into the selected memory location.

Paragraph 4.21 System Repair

"The system shall be designed to facilitate the recognition, location, replacement, repair, or adjustment of malfunctioning components or modules."

Compliance: In addition to the testing capability designed into the protection system, many failures (e.g., power, ASIC, clock, logic) of the ABRM are immediately detectable via the General Alarm incorporated into the ABRM design.

10.3 CONFORMANCE TO NRC REGULATORY GUIDES

Only certain sections of some Regulatory Guides apply to a replacement module in a Process Protection System. These are discussed in the following paragraphs:

Reg. Guide 1.75 Physical Independence of Electric Systems

Independence of Class 1E equipment and circuits is provided by the system design criteria. The section on Isolation Devices in IEEE 384 discussed in this Guide does apply to the replacement modules.

Compliance: Installation of an ABRM does not impact the plant circuit separation or redundancy requirements. The ABRM protection/control isolation capability has been demonstrated as shown in WCAP-15371, "Fault Conditions Test Report, Westinghouse ASIC-Based Replacement Module for the 7300 Process Protection System". The isolation modules were designed so that a short circuit, open circuit or the application of a credible fault on the output of the isolator will not affect the input (protective side) of the isolator.

Reg. Guide 1.89 Qualification of Class 1E Equipment for Nuclear Power Plants

IEEE 323 is discussed in this Guide. The replacement module must be seismically qualified and meet defined performance criteria during the elevated temperature conditions due to loss of the HVAC.

Compliance: Qualification of the Process Protection System is maintained when an ABRM is installed since the ABRM has been environmentally and seismically tested to the same criteria as the 7300 analog cards. The test results are reported in WCAP-15378, "Environmental Test Report, Westinghouse ASIC-Based Replacement Module for the 7300 Process Protection System", and WCAP-15215, "Seismic Test Report, Westinghouse ASIC-Based Replacement Module for the 7300 Process Protection System".

Reg. Guide 1.100 Seismic Qualification of Electric Equipment for Nuclear Power Plants

The replacement module must be seismically qualified.

Compliance: Discussed under paragraph on Reg. Guide 1.89.

Reg. Guide 1.105 Instrument Setpoints

This Regulatory Guide describes a method of ensuring that the instrumentation setpoints in systems important to safety are initially within and remain within specified limits.

Compliance: The accuracy and drift specifications of the ABRMs are bounded by the equivalent 7300 analog cards. Since they are designed to replicate the analog cards, the same ranges and spans can be obtained. Setpoints and tuning constants are entered through the Operator Interface which provides the ability to change these values by accessing memory locations. When the desired setting is obtained, the digital value representing the analog voltage is locked into the selected memory location.