GE Energy
Nuclear
3901 Castle Hayne Rd
Wilmington, NC 28401

NEDO-33288
Revision 0
Class I
DRF#0000-0065-4975
March 2007

LICENSING TOPICAL REPORT

APPLICATION OF NUCLEAR MEASUREMENT ANALYSIS AND CONTROL (NUMAC) FOR THE ESBWR REACTOR TRIP SYSTEM

INFORMATION NOTICE

This document NEDO-33288, Revision 0, contains no proprietary information.

IMPORTANT NOTICE REGARDING CONTENTS OF THIS REPORT

PLEASE READ CAREFULLY

The information contained in this document is furnished for the purpose of obtaining NRC approval of the ESBWR Certification and implementation. The only undertakings of General Electric Company with respect to information in this document are contained in contracts between General Electric Company and participating utilities, and nothing contained in this document shall be construed as changing those contracts. The use of this information by anyone other than that for which it is intended is not authorized; and with respect to **any unauthorized use**, General Electric Company makes no representation or warranty, and assumes no liability as to the completeness, accuracy, or usefulness of the information contained in this document.

TABLE OF CONTENTS

TABLE OF CONTENTS
(continued)

TABLE OF CONTENTS
(continued)

TABLE OF CONTENTS
(continued)

TABLE OF CONTENTS
(continued)

TABLE OF CONTENTS
(continued)

Abbreviations And Acronyms

Term	Definition
10 CFR	Title 10, Code of Federal Regulations
A/D	Analog-to-Digital
ac / AC	Alternating Current
ABWR	Advanced Boiling Water Reactor
ANSI	American National Standards Institute
APRM	Average Power Range Monitor
ASP	Automatic Signal Processing
ASME	American Society of Mechanical Engineers
ATWS	Anticipated Transients Without Scram
BPU	Bypass Unit
BTP	NRC Branch Technical Position
BWR	Boiling Water Reactor
CFR	Code of Federal Regulations
DAC	Design Acceptance Criteria
D/A	Digital/Analog
dc / DC	Direct Current
DCD	Design Control Document
DCIS	Distributed Control and Information System
DPS	Diverse Protection System
DTM	Digital Trip Module
EMI	Electromagnetic Interference
EPRI	Electric Power Research Institute
ESF	Engineered Safety Features
FMEA	Failure Modes and Effects Analysis
GDC	General Design Criteria

Abbreviations And Acronyms

Term	Definition
GE	General Electric Company
HVPS	High Voltage Power Supply
I&C	Instrumentation and Control
I/O	Input/Output
I&C	Instrumentation and Control
IEEE	Institute of Electrical and Electronic Engineers
INOP	Inoperable
ISO	International Standards Organization
ITAAC	Inspections, Tests, Analyses and Acceptance Criteria
LD	Load Driver
LDU	Local Display Unit
LD&IS	Leak Detection and Isolation System
LPRM	Local Power Range Monitor
MCR	Main Control Room
MSIV	Main Steam Isolation Valve
MSV	Mean Square Voltage
N-DCIS	Nonsafety-related Distributed Control and Information System
NMS	Neutron Monitoring System
NRC	Nuclear Regulatory Commission
OLU	Output Logic Unit
PRA	Probabilistic Risk Assessment
PRNM	Power Range Neutron Monitoring
Q-DCIS	Safety-related Distributed Control and Information System
RAM	Random Access Memory
RG	Regulatory Guide
RMU	Remote Multiplexing Unit

Abbreviations And Acronyms

Term	Definition
RPS	Reactor Protection System
RPV	Reactor Pressure Vessel
RTIF	Reactor Trip and Isolation Function(s)
SPTM	Suppression Pool Temperature Monitoring Sub-system of Containment Monitoring System
SRM	Staff Requirements Memoranda
SRNM	Startup Range Neutron Monitor
TLU	Trip Logic Unit
UPS	Uninterruptible Power Supply
USNRC	United States Nuclear Regulatory Commission
Vac / VAC	Volts Alternating Current
Vdc / VDC	Volts Direct Current
VDU	Video Display Unit
V&V	Verification and Validation

Explanation of Terms

Reactor Trip System	The Reactor Trip System is the term used to collectively refer to the Reactor Protection System, Neutron Monitoring System (consisting of the Startup Range Neutron Monitor, and the Power Range Neutron Monitor), and Suppression Pool Temperature Monitor. Each of these functions is designed to monitor certain parameters and cause a reactor trip if pre-determined limits are exceeded.
Reactor Protection System	The Reactor Protection System is one of the functions of the Reactor Trip System. The Reactor Protection System function is implemented in logic that resides in the RTIF system.
RTIF	RTIF is the name of the system that performs the reactor trip (i.e., RPS and SPTM) functions of the Reactor Trip System and the MSIV isolation function of the Leak Detection and Isolation System (LD&IS). RTIF is the generic name that combines the reactor trip and MSIV isolation functions into a single function. The term RTIF is always used (either explicitly or implicitly) in conjunction with a system or function. Also the name applied to the panel(s) that house(s) the NUMAC electronics that comprise the RTIF system.
NMS	NMS is the name of the system that performs the SRNM and PRNM functions of the Reactor Trip System. Also the generic name applied collectively to the safety-related and non-safety-related neutron monitoring functions, and the name applied to the panel(s) that house(s) the NUMAC electronics that comprise the NMS system.

Explanation of Terms

NUMAC	NUMAC, which stands for Nuclear Measurement Analysis and Control, is the name of the digital electronics platform (i.e., main processor, chassis, power supplies, functional modules, and software) developed by GE Energy that executes the safety-related logic for the Reactor Trip System (i.e., RPS, NMS, and SPTM), and MSIV portions of the LD&IS. The RTIF and NMS systems comprise multiple NUMAC chassis that are housed within the NMS and RTIF panels. The term NUMAC may be used to refer to the chassis, modules, and software that comprise the NUMAC system. For example, NUMAC software refers to the software that will run on the NUMAC hardware platform.
Local Display Unit	A Local Display Unit (LDU) provides a user interface display for the NUMAC system and is used primarily to perform instrument setup, diagnostics, calibration of the NUMAC electronics, and for status display. The LDU is located in the panel with the NUMAC electronics and intended to be used as maintenance display only.
Video Display Unit	A Video Display Unit (VDU) is a display located in the Main Control Room that is used by the operator. Both safety-related and nonsafety-related VDUs receive data from NUMAC systems to be displayed to the operator.

1.0 INTRODUCTION

1.1 BACKGROUND

The GE digital Nuclear Measurement Analysis and Control (NUMAC) platform has been applied in retrofits to many operating BWRs, and will be employed for the ESBWR. The NUMAC platform is a microprocessor-based system that executes application programs in firmware that is non-volatile and not changeable by the user during operation. The NUMAC platform will provide the digital monitoring and trip functions of the Reactor Trip System described in Section 7.2 of the ESBWR Design Control Document (Reference 8-6). The Reactor Trip System comprises the Reactor Protection System (RPS) function, the Startup Range Neutron Monitor (SRNM) and Power Range Neutron Monitor (PRNM) functions of the Neutron Monitoring System (NMS), and the Suppression Pool Temperature Monitoring (SPTM) function.

The safety-related NUMAC Reactor Trip and Isolation Function (RTIF) system will be used to provide the RPS automatic scram function and the MSIV automatic isolation function. As such, the RTIF system provides the combined function of RPS and portions of the Leak Detection and Isolation System (LD&IS) as well as the SPTM function.

The safety-related NUMAC Neutron Monitoring System (NMS) includes the NUMAC Startup Range Neutron Monitor (SRNM) and the NUMAC Power Range Neutron Monitor (PRNM) sub-systems. The NUMAC PRNM includes the Local Power Range Monitor (LPRM) function, the Average Power Range Monitor (APRM) function, and the Oscillation Power Range Monitor (OPRM) function.

The ESBWR is designed with four independent safety-related electrical divisions with the NUMAC RTIF actuation instrumentation employing a two-out-of-four logic scheme. The robustness of the ESBWR design is such that one division can be out of service and the protective function(s) required during and following a design basis event, including an additional single failure, can be accomplished with any two remaining divisions.

1.2 DOCUMENT SCOPE

This Licensing Topical Report (LTR) is intended to provide the information necessary to perform a licensing review and safety evaluation of the planned NUMAC application for the Reactor Trip System of the ESBWR.

The Reactor Trip System application includes the following NUMAC sub-systems:

- NUMAC RTIF, which includes the RPS automatic scram function, the MSIV automatic isolation function, and the SPTM function.
- NUMAC NMS, which includes the SRNM and PRNM monitoring and trip functions.

This LTR covers the application of each system identified above. These systems are classified as safety-related; however, some functions within these systems may be classified as nonsafety-related. Regardless, the NUMAC design and manufacturing processes for the scope covered by this LTR are similar for both safety-related and nonsafety-related systems.

The intent is to minimize the scope of review required for plant-specific applications by covering as much as feasible in the generic review.

1.3 APPLICABLE PRIOR NRC REVIEWS

The design of the RTIF and NMS systems used for the ESBWR Reactor Trip System has evolved from multiple generations of NUMAC designs, some of which have been reviewed and approved by the NRC for safety-related applications in earlier BWR plants, primarily in retrofit systems replacing the original plant equipment. A summary of the applicable prior NRC reviews is discussed below.

The prior NRC reviews for retrofit applications of the NUMAC systems were based on (a) conformance to the original design basis for the plant and (b) regulatory positions for the digital electronics at the time. For the ESBWR, the design basis and the regulatory requirements are stated in the Design Control Document (Reference 8-6).

A comparison of the NUMAC Reactor Trip System application to other NUMAC applications previously reviewed by the NRC is presented in Appendix A.

1.3.1 Startup Range Neutron Monitor

The NRC review and approval of the NUMAC SRNM, also known as the NUMAC Wide Range Neutron Monitor (WRNM), as a retrofit of the original Source Range Monitor and Intermediate Range Monitor and as a Regulatory Guide 1.97 (Reference 8-7) system in earlier BWRs, is documented in NEDO-31439A (Reference 8-2). The SRNM has been installed in over 13 BWRs worldwide. The NRC approved the WRNM implementation at the Peach Bottom Atomic Power Station Units 2 and 3 in 1997.

1.3.2 Power Range Neutron Monitor

To date, the NUMAC PRNM with OPRM has been implemented in 20 BWRs worldwide. The NRC first reviewed and approved the PRNM in NEDC-32410P-A (Reference 8-1). The NRC has also reviewed and audited various PRNM applications, with the most recent review being the implementation of the PRNM for Unit 1 of Susquehanna Steam Electric Plant.

1.3.3 ABWR

The NRC has reviewed and approved a standard design for the ABWR. The ESBWR Reactor Trip System architecture described in this LTR is derived from and is similar to the approved ABWR design.

2.0 OVERVIEW OF REACTOR TRIP SYSTEM ARCHITECTURE

2.1 GENERAL

The Reactor Trip System is a four-division, separate and redundant protection logic system framework that results in automatic trip and isolation functions. The multi-divisional trip system includes divisionally separate panels that house the equipment for controlling the various safety functions and the actuation devices. The RTIF sub-system includes the logics of the Reactor Protection System (RPS) for reactor scram and the isolation logics for the main steam-line isolation valves (MSIV). The NMS sub-system includes the logics of the SRNM and PRNM functions of the NMS.

2.2 NUMAC REACTOR TRIP AND ISOLATION FUNCTION (RTIF)

The basic system architecture of the safety-related NUMAC RTIF (i.e., the RPS and MSIV part of the LD&IS) employs four independent trip logic systems in four separate divisions of safety protection equipment. The four redundant RPS divisions are identical in design and independent in operation. There are four instrument channels provided for each process variable being monitored, one for each RPS division. Four sensors, one per division, are provided for each variable. The logic in each division does not depend on time-of-day and is asynchronous with respect to the other divisions; no division depends on the correct operation of another division or on interdivisional communication links, except as required to implement two-out-of-four voting of the individual channel trips. See Section 5.1 for a detailed description of the NUMAC components that comprise the NUMAC RTIF system.

2.3 NUMAC NEUTRON MONITORING SYSTEM (NMS)

The safety-related NUMAC NMS monitors the core neutron flux from the startup source range to beyond rated power. The NMS provides divisional two-out-of-four voted trip logic signals to the RTIF to automatically shut down the reactor when a condition requiring a reactor scram is detected.

The basic system architecture of the safety-related NUMAC NMS (i.e., the SRNM and PRNM sub-systems of NMS) employs four independent safety-related divisions of monitoring, trip, and trip logic equipment that are associated with the four RPS divisions described above. The SRNM sub-system monitors three SRNM detectors per division, and the PRNM sub-system monitors sixty-four LPRM detectors per division. As with the RTIF system, the logic in each division does not depend on time-of-day and is asynchronous with respect to the other divisions; no division depends on the correct operation of another division or on interdivisional communication links, except as required to implement two-out-of-four voting of the individual channel trips. See Section 5.2 for a detailed description of the NUMAC components that comprise the safety-related portion of the NUMAC NMS.

2.4 INTERFACES WITH OTHER SYSTEMS

The NUMAC equipment interfaces with both safety-related and nonsafety-related equipment. For example, NMS and RTIF signals are sent to the safety-related and nonsafety-related displays providing system operating status as well as trip conditions. It also sends data to the sequence of events and transient recording analysis functions. See Sections 5.1.3 and 5.2.3 for detailed descriptions of the NUMAC communication interfaces with these systems.

3.0 OVERVIEW OF REACTOR TRIP SYSTEM FUNCTIONS

3.1 RTIF FUNCTIONS

The safety function of the RTIF system is to initiate an automatic reactor trip and /or main steam isolation function whenever monitored process variables exceed or fall below (for decreasing trips) their specified trip setpoints.

The primary system functions of the safety-related NUMAC RTIF system are essentially the same as the RPS functions in most BWR plants. Section 5.1 includes detailed descriptions of the specific components in the NUMAC RTIF system that implement these functions. The primary system functions of the NUMAC RTIF for ESBWR are:

- Process input signals from various sensors, detect and reject invalid signals, filter inputs, and provide results to other functions.
- Initiate trip functions when process input signals exceed predetermined setpoints for increasing trips and fall below predetermined setpoints for decreasing trips.
- Provide outputs for operator information.
- Provide data to the plant Q-DCIS and N-DCIS systems from the RTIF, including data for Sequence of Events monitoring.
- Provide local indication and equipment status information.
- Provide an Inop alarm (non-critical) output when abnormal conditions are detected by any of the automatic testing and monitoring elements of the RTIF functions.
- Provide an Inop trip (critical) output when abnormal conditions are detected that are likely to disable one or more of the RTIF safety-related functions (including operator action to place a safety-related instrument in the Inop mode).

3.2 NMS FUNCTIONS

The primary system functions of the safety-related NUMAC NMS are summarized below. The NMS provides trip input signals to the RTIF to initiate an automatic reactor scram trip whenever monitored flux levels exceed predetermined limits. Section 5.2 includes detailed descriptions of the specific components in the NUMAC NMS that implement these functions.

3.2.1 SRNM

The SRNM monitors approximately 10 decades of neutron flux over the startup and power ranges. It operates in the counting and Mean Square Voltage (MSV) modes using a common in-

core ion chamber having a fissionable and regenerative emitter to cover all of the ranges, and a microprocessor-based NUMAC monitor to calculate the reactor parameters. The primary system functions of the NUMAC SRNM for the ESBWR are:

- Calculate reactor power and period over 10 decades using the measurements from a breeder type neutron sensitive ion chamber.
- Provide continuous monitoring of rector power level from 10E-9% to 10E+2% power in compliance with the requirements of RG 1.97 (Reference 8-7).
- Provide power and period output data to the plant Q-DCIS and N-DCIS systems and for operator information.
- Provide alarm, trip, and control rod block signals.
- Provide automatic self-calibration and self-testing of the SRNM and the preamplifier.
- Provide compensation of the detector sensitivity based on the life of detector.
- Provide an Inop alarm (non-critical) output when abnormal conditions are detected by any of the automatic testing and monitoring elements of the SRNM functions.
- Provide an Inop trip (critical) when abnormal conditions are detected that are likely to disable one or more of the SRNM safety-related functions (including operator action to place a safety-related instrument in the Inop mode).

3.2.2 PRNM

The PRNM monitors neutron flux over the power range, from 1% power to beyond rated power. The primary system functions of the NUMAC PRNM system include the LPRM function, APRM function, and OPRM function to detect and suppress thermal hydraulic instability. These functions are essentially the same as the safety-related power range neutron monitoring functions in most BWR plants. The primary system functions of the NUMAC PRNM for the ESBWR are:

- Provide polarizing voltage to LPRM detectors.
- Process input signals from LPRM detectors, detect and reject invalid signals, filter inputs, apply gain adjustments previously calculated and supplied from the plant computer, and provide results to other functions.
- Combine processed LPRM detector signals in groups (one per APRM) previously defined into independent core average neutron flux levels, normalize and adjust the average to read in units of percent of rated core thermal power based on calibration factors previously calculated and supplied from the plant computer.
- Derive Simulated Thermal Power based on measured, average neutron flux.
- Compare normalized and adjusted average neutron flux values to predefined fixed setpoints and generate scram or rod block signals when setpoints are exceeded.

- Compare calculated Simulated Thermal Power to predetermined values and generate scram or rod block signals when setpoints are exceeded.
- Apply the OPRM detect-and-suppress algorithms to the LPRM signals and provide a trip output when the oscillation trip criteria are exceeded.
- Provide outputs for operator information and displays.
- Provide data to the plant Q-DCIS and N-DCIS systems from the PRNM.
- Provide an Inop alarm (non-critical) output when abnormal conditions are detected by any of the automatic testing and monitoring elements of the PRNM functions.
- Provide an Inop trip (critical) when abnormal conditions are detected that are likely to disable one or more of the PRNM safety-related functions (including operator action to place a safety-related instrument in the Inop mode).

4.0 DESIGN BASES AND CONFORMANCE WITH REGULATORY REQUIREMENTS

4.1 DESIGN BASES

The safety-related and nonsafety-related design bases for the NUMAC platform for the ESBWR are described in the ESBWR Design Control Document (Reference 8-6).

4.2 CONFORMANCE WITH REGULATORY REQUIREMENTS

The following Regulatory Requirements, as outlined in 26A6642AW, are applicable to the NUMAC platform for ESBWR:

4.2.1 10 CFR 50.55a (Codes and Standards)

10 CFR 50.55a(a)(1) and 50.55a(h) are applicable to the NUMAC instrumentation. 10 CFR 50.55a(h) requires the application of IEEE Std. 603-1991 for protection systems. For application in ESBWR, the IEEE requirement will be addressed through IEEE Std. 603, a position endorsed in Regulatory Guide 1.153.

4.2.2 10 CFR 50.34(f) (Conformance with TMI Action Plan Requirements)

This is not applicable to the application of the NUMAC platform for ESBWR.

4.2.3 Other 10CFR

- **10 CFR 50.62 (ATWS)**
  - The NUMAC NMS provides an ATWS Permissive output to enable the ATWS function. The ATWS logic is implemented in equipment that is diverse from the microprocessor based NUMAC RTIF equipment that provides the RPS function.
- **10 CFR 52.47(a)(1)(iv) Resolution of Unresolved and Generic Safety Issues**
  - Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11 of the ESBWR Design Control Document (Reference 8-6).
- **10 CFR 52.47(a)(1)(vi) ITAAC in Design Certification Applications**
  - Conformance: ITAAC are provided for the ESBWR I&C systems and equipment in DCD Tier 1 (Reference 8-9) and are applicable to the NUMAC platform.
- **10 CFR 52.47(a)(1)(vii) Interface Requirements**
  - Conformance: No interface requirements are applicable to the NUMAC platform.

- **10 CFR 52.47(a)(2) Level of Detail**
  - Conformance: The level of detail provided in this document conforms to this code and is applicable to the NUMAC platform.
- **10 CFR 52.47(b)(2)(i) Innovative Means of Accomplishing Safety Functions**
  - Conformance: The ESBWR is not designed with innovative means of accomplishing safety functions. See Section 7.1.6.1 of DCD (Reference 8-6).
- **10 CFR 52.79(c), ITAAC in Combined License Applications**
  - Conformance: Not applicable to the NUMAC platform standard design.
- **10 CFR 50 Appendix A, General Design Criteria (GDC):**
  - Conformance with NRC General Design Criteria (10 CFR 50 Appendix A) is discussed in Section 3.1 of the DCD (Reference 8-6) for ESBWR. The applicability of GDC to each system is presented in Table 7.1-1 of the DCD.

4.2.4 Staff Requirements Memoranda (SRM)

- **SRM to SECY 93-087 II.Q (Defense Against Common-Mode Failures):**
  - The NUMAC platform is designed to meet the defense-in-depth and diversity requirements for defense against common-mode failures for the ESBWR digital I&C.
- **SRM to SECY 93-087 II.T (Control Room Annunciator/Alarm Reliability)**
  - Section II.T of SECY 93-087 applies specifically to the post-accident monitoring requirement, which is applicable to the SRNM sub-system in the NUMAC NMS.

4.2.5 Conformance to Regulatory Guides

A discussion of the general conformance of the NUMAC platform with Regulatory Guides follows. Individual system conformance, along with any clarifications or exceptions, is addressed in the Safety Evaluation subsections within Sections 7.1 through 7.8 of the DCD (Reference 8-6).

- **Regulatory Guide 1.22, Periodic Testing of Protection System Actuation Functions**
  - This includes conformance with BTP HICB-8. The equipment in the NUMAC platform is capable of being tested during plant operation from sensor device to final actuator device. The tests must be performed in overlapping stages so that an actual safety function, e.g., reactor scram, would not occur as a result of the testing.
- **Regulatory Guide 1.47, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems**
  - This Regulatory Guide is applicable to the NUMAC platform that is designed to provide the following:

- Automatic indication that a system is out of service is provided in the control room. Devices indicate which part of a system is not operable.
- A manual switch with mutually exclusive positions for each channel is provided for manual bypass actuation, which annunciates out-of-service conditions.
- Display provisions serve to supplement administrative controls and aid the operator in assessing the availability of component and system level protective actions. These displays do not perform safety-related functions.
- System out-of-service alarm circuits are electrically isolated from the plant safety-related systems to prevent adverse effects.
- Testing is included on a periodic basis, when equipment associated with the display is tested.

- **Regulatory Guide 1.53, Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems**
  - Compliance with NRC Regulatory Guide 1.53 is satisfied by specifying, designing, and constructing the NUMAC systems to meet the single-failure criterion, Section 5.1, of IEEE 603, Standard Criteria for Safety Systems for Nuclear Power Generating Stations with any three of the four divisions of safety-related power available. Four divisional redundant sensors physically separated from each other provide inputs to the four divisional RMU panels. The RMU panels are located in four physically separate safety-related rooms. All divisional cables are physically separated and isolated from each other as well as from other nonsafety-related cables. In the DCIS rooms, the RTIF and NMS equipment are housed in divisional safety-related panels again physically isolated from each other and from nonsafety-related equipment. Interfaces between divisions, limited to signals required to accomplish the two-out-of-four logic are isolated through the use of fiber optic cables.
- **Regulatory Guide 1.62, Manual Initiation of Protective Actions**
  - Means are provided for manual initiation of reactor scram through the use of two armed pushbutton switches and the reactor mode switch by safety actions through appropriate switches. Reactor scram is accomplished by operation of both pushbutton switches, or by placing the mode switch in the SHUTDOWN position. These switches are located on the main control console.
  - Means are also provided for the manual initiation of the ATWS function through operation of two armed pushbutton switches located on the main control console.
  - The equipment common to initiation of both manual scram and automatic scram is limited to actuator load power sources, actuator loads and cabling between the two. There is no shared trip or scram logic equipment for manual scram and automatic scram. No single failure in the manual, automatic, or common portions of the protection system would prevent initiation of reactor scram by manual or automatic means with any three of the four divisions of safety-related power available.

- Manual initiation of reactor scram, ATWS or other safety functions, once initiated, goes to completion as required by IEEE 603, Section 5.2.

- **Regulatory Guide 1.75, Physical Independence of Electric Systems**
  - The NUMAC platform complies with the criteria set forth in IEEE 603, Section 5.6, and Regulatory Guide 1.75, which endorses IEEE Std. 384. Safety-related circuits and associated circuits are identified and separated from redundant and nonsafety-related circuits. Isolation devices are provided where an interface exists between redundant safety-related divisions and between safety-related or associated circuits and nonsafety-related circuits.
  - Physical and electrical independence of the instrumentation devices of the system is provided by channel independence for sensors exposed to each process variable. Separate and independent raceways are routed from each device to the respective data acquisition and signal conditioning units (i.e., Remote Multiplexing Unit). Each channel utilizes its own divisional separate and independent electronic equipment located in separate equipment rooms. Trip logic outputs are separated in the same manner as the channels. Fiber optic cables are used where it is necessary for trip signals to cross divisions for two-out-of-four logic. The fiber optic cables provide the electrical isolation between divisions. Nonsafety-related circuits for lights and utility power are separated from safety-related circuits in the safety-related panels and are routed in grounded metal conduit.

- **Regulatory Guide 1.97 - Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident**
  - The SRNM conforms with Regulatory Guide. 1.97.

- **Regulatory Guide 1.105, Instrument Setpoints for Safety-Related Systems**
  - The initiation setpoints for the safety-related systems in the NUMAC platform are established consistent with this guide. A future licensing topical report, NEDO-33294 (Reference 8-8) will provide a detailed description of this methodology.

- **Regulatory Guide 1.118, Periodic Testing of Electric Power and Protection System**
  - The NUMAC RTIF complies with RG 1.118 as amplified in IEEE 338. The RTIF is designed so that its individual elements can be periodically and independently tested to demonstrate that the system reliability is being maintained. Safety-related RTIF equipment allows for inspection and testing during periodic shutdowns and refueling.

- **Regulatory Position C.5 for APRM**
  - With respect to conformance with position C.5, the inherent time response of the in-core sensors used for the APRM function (fission detectors operating in the ionization chamber mode) is many orders of magnitude faster than the APRM channel signal conditioning electronics and response time requirements. The sensors cannot be tested without disconnecting and reconnecting to special equipment.

- **Regulatory Guide 1.152, Criteria for Digital Computers in Safety Systems of Nuclear Power Plants**
  - The NUMAC platform complies with this Regulatory Guide. The NUMAC RTIF and NUMAC NMS hardware and software are developed in compliance with this Regulatory Guide, which endorses IEEE Std. 7-4.3.2 and IEEE Std. 603. The structured development plan for NUMAC controllers includes conformance with the software standards referenced in IEEE Std. 7-4.3.2. Hardware and software (firmware) are integrated into a final assembly that is validated by testing against input requirements. The NUMAC firmware is developed in accordance with the ESBWR Software Management Plan (Reference 8-16) and the ESBWR Software Quality Assurance Plan (Reference 8-17). The NUMAC firmware resides in non-volatile memory and cannot be altered by the user.
- **Regulatory Guide 1.153, Criteria for Power, Instrumentation, and Control Portions of Safety Systems**
  - The NUMAC Reactor Trip System configuration in meeting independence and separation requirements, and the single-failure criterion for the RPS function and other safety-related systems, conforms with the requirements of this Regulatory Guide that endorses IEEE-Std. 603.
- **Regulatory Guide 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants**
  - The NUMAC platform conforms with this Regulatory Guide that endorses IEEE Std. 1012, IEEE Standard for Software Verification and Validation Plans, and IEEE Std. 1028, IEEE Standard for Software Reviews and Audits. IEEE Std. 1012 is acceptable for providing high functional reliability and design quality in software used in safety-related systems. IEEE Std. 1028 is acceptable for carrying out software reviews, inspections, walkthroughs, and audits subject to certain provisions. The NUMAC software development for the Reactor Trip System of the ESBWR uses the guidance in these standards discussed in DCD (Reference 8-6) Appendix 7B to develop portions of the overall software development plan and thus complies with this regulatory guide.
- **Regulatory Guide 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants**
  - The NUMAC platform conforms with this Regulatory Guide that endorses IEEE Std. 828, IEEE Standard for Software Configuration Management Plans, and ANSI/IEEE Std. 1042, IEEE Guide to Software Configuration Management. These standards, with the clarifications provided in the Regulatory Position, describe acceptable methods for providing high functional reliability and design quality in software used in safety-related systems. The NUMAC software development for the ESBWR uses the guidance in these standards discussed in DCD (Reference 8-6) Appendix 7B to develop portions of the overall software development plan and thus complies with this regulatory guide.

- **Regulatory Guide 1.170 - Software Test Documentation For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants**
  - The NUMAC platform conforms with this Regulatory Guide that endorses the requirement contained in IEEE Std. 829, IEEE Standard for Software Test Documentation, that provides an acceptable approach for meeting the requirements of 10 CFR Part 50 as they apply to the test documentation of safety-related system software subject to the provisions in this guide. The NUMAC software development for the ESBWR uses the guidance in these standards discussed in DCD (Reference 8-6) Appendix 7B to develop portions of the overall software development plan and thus complies with this regulatory guide.
- **Regulatory Guide 1.171 - Software Unit Testing For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants**
  - The NUMAC platform conforms with this Regulatory Guide that endorses IEEE Std. 1008, IEEE Standard for Software Unit Testing, subject to the provisions in this guide. This standard defines an acceptable method for planning, preparing for, conducting, and evaluating software unit testing. The NUMAC software development for the ESBWR uses the guidance in these standards discussed in DCD (Reference 8-6) Appendix 7B to develop portions of the overall software development plan and thus complies with this regulatory guide.
- **Regulatory Guide 1.172 - Software Requirements Specifications For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants**
  - The NUMAC platform conforms with this Regulatory Guide that endorses IEEE Std. 830, Recommended Practice for Software Requirements Specifications, as amended in the Regulatory Position. This standard describes current practice for writing software requirements specifications for a wide variety of systems. It is not specifically aimed at safety-related applications; however, it does provide guidance on the development of software requirements specifications that will exhibit characteristics important for developing safety-related system software. This is consistent with the goal of ensuring high-integrity software in reactor safety-related systems. The NUMAC software development for the ESBWR uses the guidance in these standards discussed in DCD (Reference 8-6) Appendix 7B to develop portions of the overall software development plan and thus complies with this regulatory guide.
- **Regulatory Guide 1.173 - Developing Software Life Cycle Processes For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants**
  - The NUMAC platform conforms with this Regulatory Guide that endorses IEEE Std. 1074. The standard describes, in terms of inputs, development, verification or control processes, and outputs, a set of processes and constituent activities that are commonly accepted as composing a controlled and well coordinated software development process. It describes inter-relationships among activities by defining the source activities that produce the inputs and the destination activities that receive the

outputs. The standard specifies activities that must be performed and their inter-relationships; it does not specify complete acceptance criteria for determining whether the activities themselves are properly designed. Therefore, the standard should be used in conjunction with guidance from other appropriate regulatory guides, standards, and software engineering literature. The NUMAC software development for the ESBWR uses the guidance in these standards discussed in DCD (Reference 8-6) Appendix 7B to develop portions of the overall software development plan and thus complies with this regulatory guide.

- **Other US NRC Regulatory Guides**
  - The following additional US NRC Regulatory Guides, identified as part of the basis for the currently installed NUMAC systems at some plants, either are or can be applied when compliance is determined by actions outside the scope of the application to the ESBWR designs as described in this LTR:
    - Reg. Guide 1.29, Rev. 3, Seismic Design
    - Reg. Guide 1.63, Rev. 3, Electrical Penetration Assemblies in Containment Structures for Nuclear Power Plants
    - Reg. Guide 1.68, Rev. 2, Initial Test Programs for Water-Cooled Nuclear Power Plants
    - Reg. Guide 1.70, Rev. 3, Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants

4.2.6 Branch Technical Positions

- **BTP HICB-3:** Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service – The ESBWR has no reactor coolant pump and the BTP Position One does not apply. The ESBWR complies with the BTP Position Two.
- **BTP HICB-8:** Guidance for Application of Regulatory Guide 1.22 – The NUMAC RPS for ESBWR design conforms with this BTP as discussed in the compliance with RG 1.22 in the DCD (Reference 8-6).
- **BTP HICB-9:** Guidance on Requirements for Reactor Protection System Anticipatory Trips —The NUMAC hardware used to provide trip signals in the RPS is designed in accordance with IEEE 603, is safety-related, and meets Seismic Category I requirements.
- **BTP HICB-11:** Guidance on Application and Qualification of Isolation Devices— The NUMAC platform design conforms with this position. The NUMAC equipment (i.e., NMS and RTIF) uses fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections between safety-related and nonsafety-related devices.

Certain diverse and hardwired portions of RPS may use coil-to-contact isolation of relays or contactors. This is acceptable according to the BTP when the application is analyzed or tested per the guidelines of Reg. Guide 1.75 and Reg. Guide 1.153.

- **BTP HICB-12:** Guidance on Establishing and Maintaining Instrument Setpoints – The NUMAC platform conforms with this position. The safety-related system trip setpoints (i.e., RPS, NMS) will be consistent with the requirements of Regulatory Guide 1.105. The setpoints will be established based on instrument accuracy, calibration capability and design drift (estimated) allowance data, and will be within the instrument best accuracy range. The digital NUMAC trip setpoints do not drift and are reported to the N-DCIS to be alarmed for any change; the analog to digital converters are self calibrating and the NUMAC instruments uses self diagnostics that are reported to the N-DCIS through isolated gateways. It is expected that the variability in the parameter channel will be attributable to the field sensor. The established setpoints will provide margin to satisfy both safety requirements and plant availability objectives.
- **BTP HICB-13:** Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors - The NUMAC RTIF uses sensor inputs for suppression pool temperature monitoring, which is based on thermocouple type temperature sensors for trip application, and are not used for continuous temperature measurement. This BTP does not apply to RTIF.
- **BTP HICB-14:** Guidance on Software Reviews for Digital Computer-based Instrumentation and Control Safety Systems
- Development of software for the safety-related system functions within NUMAC RTIF and NMS conforms with the guidance of this BTP. Discussion of software development is included in Appendix 7B to the DCD (Reference 8-6). Safety-related software to be embedded in the memory of the NUMAC RTIF and NMS safety-related controllers is developed according to a structured plan. These plans follow the software life cycle process described in the BTP.
- **BTP HICB-16:** Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52 - This BTP is applicable to all sections of the DCD (Reference 8-6).
- **BTP HICB-17:** Guidance on Self-Test and Surveillance Test Provisions in Digital Computer-based Instrumentation and Control Systems. The NUMAC RTIF and NMS safety-related controllers conform with this BTP.
- **BTP HICB-18:** Guidance on Use of Programmable Logic Controllers in Digital Computer-based Instrumentation and Control Systems

  NUMAC does not use Programmable Logic Controllers (PLCs).
- **BTP HICB-19:** Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems (Item II.Q of SECY-93-087) – The ESBWR Reactor Trip System design conform with this BTP by the implementation

of an additional diverse instrumentation and control system, the DPS, described in Section 7.8 of the DCD (Reference 8-6).

- **BTP HICB-21:** Guidance on Evaluation of Digital System Architecture and Real-Time Performance

  The real-time performance of the NUMAC RTIF and NMS safety-related systems in meeting the requirements for safety-related system trip and initiation response conforms with this BTP. Each NUMAC controller operates independently and asynchronously with respect to other controllers so that timing can readily be evaluated from input to output of each controller. Timing signals are not exchanged between divisions of independent equipment or between controllers within a division.

4.2.7 Conformance with Industry Standards IEEE Std. 323 and IEEE Std. 344

The instruments in the NUMAC platform conform with the following industry standards:

IEEE Std. 323 - Qualifying Class 1E Equipment for Nuclear Power Generating Stations - Safety-related systems are designed to meet the requirements of IEEE Std. 323.

IEEE Std. 344 - Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations - Safety-related instrumentation and control equipment is classified as Seismic Category I and designed to withstand the effects of the safe shutdown earthquake (SSE) and remain functional during normal and accident conditions. Qualification and documentation procedures used for Seismic Category I equipment and systems satisfy the provisions of IEEE Std. 344.

4.2.8 Conformance with IEEE Std. 603

IEEE Std. 603 is endorsed by Reg. Guide 1.153. The NUMAC safety-related systems comply with IEEE Std. 603.

4.2.8.1 Single Failure Criterion (IEEE-603, Section 5.1)

This section requires that any single failure within the safety system shall not prevent proper protective action at the system level when required, and it should be confirmed that requirements of the single failure criterion are satisfied. The NUMAC safety-related systems for ESBWR satisfy the single failure criterion even with only three of the four divisions of safety-related power available. All NUMAC safety-related systems have multiple (four) redundant and independent channels, including redundant and independent sensors assigned to each of the redundant channels. The trip logic is two-out-of-four. Any failed channel caused by a single failure associated with this channel, in addition to one of four divisions out of service (or bypassed), does not prevent the safety system from performing its safety protection functions because of this two-out-of-four logic. The failed channel in addition to one of four divisions out of service (or bypassed) will not affect the performance of the safety system functions, with the logic continuing to provide the requisite two channels to initiate the protective action.

4.2.8.2 Completion of Protective Action (IEEE Std. 603, Section 5.2)

Completion of a protective action, once initiated automatically or manually, is accomplished by the NUMAC safety-related systems with seal-in logic.

4.2.8.3 Quality (IEEE Std. 603, Section 5.3)

NUMAC equipment is provided under GE's Appendix B quality program. The NRC accepted the GE Quality Assurance Program (Reference 8-5) with its implementing procedures that constitute the Quality Assurance system applied to the GE NUMAC safety-related system design. It satisfies applicable requirements of the following: (1) 10 CFR 50 Appendix B; (2) ANSI/ASME NQA-1; (3) ISO 9001, and complies with IEEE Std. 603, Section 5.3.

4.2.8.4 Equipment Qualification (IEEE Std. 603, Section 5.4)

Safety-related system equipment is designed to meet the functional performance requirements over the range of normal environmental conditions for the area in which it is located. Equipment qualification typically includes electromagnetic interference qualification, seismic qualification, and other environmental condition qualification such as temperature, humidity, radiation, and pressure. The NUMAC safety systems are designed to meet the equipment qualification requirements set forth in IEEE Std. 603, Section 5.4, and other associated equipment qualification requirements. The qualification was established using qualification methods set forth in the General Electric Qualification Program (Reference 8-3). The NUMAC safety-related system components are qualified to operate in the normal and abnormal environments in which they are located. Additional discussion of the Equipment Qualification is provided in Section 4.3.

EMI Qualification: The NUMAC safety-related components, when mounted in accordance with the specified mounting methods, are designed to be qualified by type testing and analysis to demonstrate that the components will perform all specified functions correctly when operated within the specified EMI limits. The NUMAC safety-related equipment is designed to be not susceptible to electromagnetic disturbances from neighboring modules and does not cause electromagnetic disturbances to neighboring modules. The EMI qualification design follows the requirements specified in MIL-STD-461D (Reference 8-10), MIL-STD-462D (Reference 8-11), and IEC Standard 61000-4 (Reference 8-12), depending upon the specific requirement conditions. The NUMAC safety-related equipment is to be qualified to perform within its specifications continuously while exposed to EMI environmental limits at the hardware mounting location. EPRI Report TR-102323 (Reference 8-4) is used to establish the envelope limits. The EMI susceptibility and emissions testing is performed by type testing. In addition to the equipment design considerations, plant-specific actions are required to establish practices to control emission sources, maintain good grounding practices, and maintain equipment and cable separation.

4.2.8.5 System Integrity (IEEE Std. 603, Section 5.5)

The safety-related I&C systems are required to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis. Other areas that are necessary to address as requirements include adequate system real-time performance for digital computer-based systems to ensure completion of protective action, evaluation of hardware integrity and software integrity (software safety analysis, as part of BTP HICB-14 requirements), fail in a safe state upon loss of energy or adverse environmental conditions, and the requirements for manual reset.

The NUMAC safety-related systems meet the integrity requirements described in IEEE Std. 603, Section 5.5. The Reactor Trip System functions for ESBWR fail in the tripped state. For the ESBWR RTIF functions, detection of an inoperable input instrument will lead to channel trip. Hardware and software failures detected by self-diagnostics will cause trip actuation. Also, failure of hardware and software will not inhibit manual initiation of protective functions.

4.2.8.6 Independence (IEEE Std. 603, Section 5.6)

The independence requirements of IEEE Std. 603, Section 5.6, address the independence between redundant portions of a safety-related system, between the safety-related systems and the effects of design basis events, and between the safety-related systems and other systems. Three aspects of independence are addressed in each case, i.e., physical independence, electrical independence, and communication independence. The NUMAC safety-related systems meet these requirements. These systems have four redundant and independent channels, which are physically independent and separated, with independent electrical power source applied to each channel. There are no common switches shared by the four channels. The sensors used for each of the four channels are independent and physically separated from one another. Communications directly between the four channels are limited to channel trip signals and bypass status signals, and are through proper isolation devices using optical fibers.

Independence requirements between the safety-related systems and the effects of design basis events are achieved through proper equipment qualification. The NUMAC safety equipment is qualified for continuous functional capability for the environment and location in which the equipment is located and where design basis event conditions are considered. The NUMAC safety systems are totally separated and independent from nonsafety-related systems. Communication from safety-related systems to nonsafety-related systems is carried out with proper signal isolation devices (i.e., fiber optic cables) and a data path gateway. Communication from nonsafety systems to safety systems is prohibited, with two exceptions: 1) the on-demand transmission of LPRM and APRM calibration gain adjustment factors (which are calculated in the nonsafety-related plant computer function of the N-DCIS) to the safety-related PRNM equipment using proper signal isolation and administrative controls, and 2) the periodic transmission of time-of-day (used for display and time tagging of data) from the N-DCIS to the safety-related NUMAC Reactor Trip System equipment using proper signal isolation and data buffering techniques. This transmission of data from nonsafety-related systems to safety-related

systems does not interfere with RPS protection functions. Additional discussion of these communication interfaces is provided in Sections 5.1.3 and 5.2.3.

4.2.8.7 Capability for Testing and Calibration (IEEE Std. 603, Section 5.7)

The capability for testing and calibration of safety-related system equipment is required to be provided during power operation and is required to duplicate the performance of the safety-related function as closely as practicable. It is permitted that tests be performed in overlapping test segments in order to test one safety-related function. Also, the I&C design should allow for tripping or bypass of individual functions in each safety system channel. The NUMAC safety systems meet the requirements as outlined in IEEE Std. 603, Section 5.7. The functions of each safety-related channel can be tested on line with the tested channel bypassed from the two-out-of-four trip logic. The NUMAC equipment has built-in self-diagnostic functions to identify critical failures such as loss of power and data errors, etc.

4.2.8.8 Information Displays (IEEE Std. 603, Section 5.8)

Displays for manually controlled actions: Type A variables are those that provide the primary information required for the control room operators to take the specified manual actions for which no automatic control is provided and that are required for safety-related systems to accomplish their safety functions for design basis accident events. For NUMAC there are no Type A variables.

- **System Status Indication:** The NUMAC instruments support the ESBWR design goal of providing safety-related and nonsafety-related I&C systems with system status information that meet the requirements of IEEE Std. 603, Section 5.8. Pertinent system trip/logic status, parameter data values, equipment functional status, and actuator status are available to be displayed to the operator upon request. For safety-related systems, such information is available for each division/channel. Information important to plant operation and status monitoring is permanently displayed (on large wide display panels) in the MCR. Alarm (and annunciation) indications are also available in the MCR per system design requirements. Other than post-accident safety-related displays, the system status information is not safety-related.
- **Indication of Bypasses:** For safety-related system protection functions, bypass status of a NUMAC instrument is continuously displayed to the operator. All bypass status information is available to be displayed per system design requirements. Bypass information is accompanied with an alarm when activated under abnormal conditions.
- **Location of Display:** Displays in the MCR are either on the main control console or on the large wide display panels visible and accessible to the operator. The ESBWR man-machine interface system design (human system interface) includes design requirements and specifications for the classification of locations of displays in the MCR.

4.2.8.9 Control of Access (IEEE Std. 603, Section 5.9)

The NUMAC instrument is protected by keylock switch and password for access control and is in full compliance with IEEE Std 603, Section 5.9. Only qualified plant personnel are allowed to exercise operations such as change of setpoints, instrument calibration, equipment testing, logic bypass operation, and access to other plant operation switches. Software of the NUMAC safety systems is not changeable at the plant site as the safety-related system software is implemented as firmware in a microprocessor. There is no access to safety-related system equipment and control functions via any network from nonsafety-related system equipment.

4.2.8.10 Repair (IEEE Std. 603, Section 5.10)

The NUMAC safety-related systems are designed to allow the timely recognition (such as by periodic self-diagnostic functions) of failures, including component location, replacement requirements (such as through module replacement), repair and adjustment of malfunctioning equipment. The self-diagnostic functions will locate the failure to the component level. Through individual channel bypassing, the failed component can be replaced or repaired on line without affecting the safety-related system protection function, with the trip logic amended from two-out-of-four to two-out-of-three. The single failure criterion is still met even with only three of the four divisions of safety-related power available during repair, including bypassing, by continuing to provide the requisite two channels to initiate the protective action.

4.2.8.11 Identification (IEEE Std. 603, Section 5.11)

The NUMAC safety-related system equipment satisfies the identification requirements specified in IEEE Std. 603, Section 5.11. The NUMAC safety-related system equipment is distinctly identified for each redundant portion of a safety-related system with identifying markings. For digital computer-based system equipment, different versions of computer hardware, programs, and software are distinctly identified. Configuration management is implemented to assist system program and software identification. All NUMAC hardware components or equipment units have identification labels or nameplates.

4.2.8.12 Auxiliary Features (IEEE Std. 603, Section 5.12)

The ESBWR safety I&C system auxiliary supporting features satisfy the requirements of IEEE Std. 603, Section 5.12 where applicable, such as safety-related electrical system equipment including batteries and inverters.

4.2.8.13 Multi-Unit Stations (IEEE Std. 603, Section 5.13)

The ESBWR standard design submitted for NRC certification is a single-unit plant.

4.2.8.14 Human Factors Considerations (IEEE Std. 603, Section 5.14)

In the ESBWR I&C design, human factors are considered at the outset and throughout the design process, following the necessary regulatory and design guidelines (e.g., NUREG-0711), to assure that safety-related system design goals are met. The design of the NUMAC equipment meets the intent of NUREG-0700 as applicable to the back panel equipment.

4.2.8.15 Reliability (IEEE Std. 603, Section 5.15)

The degree of redundancy, diversity, testability, and quality of the NUMAC I&C design is adequate to achieve the functional reliability necessary to perform its function. All equipment is provided under GE's Appendix B quality program. BTP-14 will be followed for software development processes to achieve reliable software design and implementation. Design measures to achieve defense against common mode failure have been included in the safety I&C design through many defense-in-depth and diversity measures including the incorporation of the Diverse Protection System described in ESBWR I&C Defense-in-Depth and Diversity Report (Reference 8-14). The NUMAC safety-related systems are included in the consideration of the ESBWR Probabilistic Risk Assessment (PRA), referenced in Chapter 19 of the DCD (Reference 8-6).

4.2.8.16 Sense, Command, and Execute Features per IEEE Std. 603

- Automatic and Manual Control (IEEE Std. 603, Sections 6.1, 6.2, 7.1, and 7.2)

  The NUMAC safety-related systems for ESBWR are designed to automatically initiate a reactor scram trip and actuate the engineered safety features to mitigate the consequences of anticipated operational occurrences and design basis accidents. Such automatic protection actions are implemented via a two-out-of-four voting (of four divisions) whenever one or more process variables monitored and measured by the RTIF or NMS logics (in any two of the four divisions) reach the scram setpoint. In the setpoint determination, an appropriate setpoint value is selected for each process variable based upon GE setpoint methodology (Reference 8-15) that includes margins and errors. Appropriate instrument and equipment response times are also considered in the safety analyses.

  The manual initiation of protective functions of a NUMAC instrument at the system-level and division level is available. The manual controls are designed such that the information provided and display content and location are taken into consideration for easy operator access and action in the MCR. No single failure will prevent the initiation of the protection action with any three of the four divisions of safety-related power available.

- Interaction Between the Sense and Command Features and Other Systems (IEEE Std. 603, Section 6.3)

The NUMAC safety-related systems are totally separate and independent from the nonsafety-related control systems such that any failure of nonsafety-related systems will not affect and will not prevent the NUMAC safety protection system from performing its safety-related protection functions. Sensors used by safety NUMAC systems are not shared by nonsafety-related control systems. The NUMAC safety-related systems meet the requirements of GDC 24. (The only interface from a nonsafety-related system to safety-related I&C is the data transmission of LPRM and APRM gain adjustment factor data from the plant computer system to the PRNM units. However, such data transmission to PRNM units requires operator acknowledgment for implementation, and does not interfere with reactor protection functions or ESF actuation functions.)

- Derivation of System Inputs (IEEE Std. 603, Section 6.4)

  To the extent feasible, the protection system inputs are derived from signals that directly measure the designated process variables. The SRNM system inputs are from the SRNM detectors. The inputs for the APRM are from the LPRM detectors. Where applicable, these systems provide direct input to the RPS. The only two RPS sensing inputs that are not direct measures of the variables are the reactor pressure vessel (RPV) water level and the loss of feedwater flow in the RPS scram logics. The RPV water level is measured by the delta pressure derived from the sensing line with a reference point. This method is a proven technology in BWR applications. The loss of feedwater flow variable is represented by the loss of power generation bus signal, because when the power to the feedwater pump motor is lost, the feedwater flow also is lost. The use of the loss of power generation bus signal to represent the loss of feedwater flow signal meets the requirements of the Safety Analysis of Chapter 15 of the DCD (Reference 8-6).

- Capability for Testing and Calibration (IEEE Std. 603, Section 6.5)

  NUMAC instruments are designed such that they can be tested, inspected, and calibrated as required during plant operation without causing plant shutdown or scram, and with easy access to the service personnel. The NUMAC instrument modules, such as SRNM and APRM, are designed with the capability of being tested for normal performance, trip performance, and calibration function, through either an automated or manual process. Routine surveillance functions, including periodic tests and calibration, are automated with minimum operator involvement.

  Detailed NUMAC instrument test function requirements, including periodic tests and calibration durations for each instrument, will be included in the detailed NMS hardware and software system specification document.

  For RTIF, the operational availability of the protection system sensors can be checked by perturbing the monitored variables, by cross-checking between redundant channels that bear a known relationship with each other and that have read-outs available, or by introducing and varying a substitute input to the sensor of the same nature as the measured variable.

For microprocessor-based instruments, an instrument unit self-test function is provided. Limited self-test capability is also provided for NUMAC instruments that are non-microprocessor based.

- Operating Bypasses (IEEE Std. 603, Sections 6.6 and 7.4)

  The NUMAC RTIF and NMS safety-related systems are designed with operating bypasses. One example of such operating bypasses is associated with the trip function dependence on reactor operating mode. Requirements of IEEE Std. 603 are met by the NUMAC operating bypass design.

- Maintenance Bypass (IEEE Std. 603, Sections 6.7 and 7.5)

  The NUMAC safety-related systems are designed with maintenance bypass capability. This is mainly for the purpose of equipment maintenance, testing, and repair of one individual division (channel) with the plant operating and without initiating any protection functions. The single failure criterion is met under such a bypass condition even with only three of the four divisions of safety-related power available. A maintenance bypass is always indicated in the MCR. Maintenance bypass for NUMAC safety-related systems is applied through a joystick bypass switch (with exclusive logic) where only one channel (out of four channels) is allowed to be bypassed at any given time. In the case of the SRNM, the 12 SRNM channels are divided into four bypass groups and only one sensor in each group can be bypassed at a time. A Technical Specification will define the time duration for which a specific maintenance bypass condition is allowed to exist in any of the three required safety-related divisions. Since the safety design basis is met with any three of four divisions, bypass or maintenance on one of the four divisions is administratively controlled and not expressly limited by Technical Specifications. Maintenance bypasses are initiated manually by the plant operator per administrative control.

- Setpoints (IEEE Std. 603, Section 6.8)

  The ESBWR Safety-Related I&C system setpoints are defined, determined, and implemented based on the GE setpoint methodology (Reference 8-15) approved by the NRC. This methodology meets the requirements of IEEE Std. 603 and is used to determine the setpoints for the NUMAC safety-related systems. The setpoints are stored in non-volatile memory and can only be altered under keylock and password protected administrative control.

- Power Source Requirements (IEEE Std. 603, Sections 8.1 and 8.2)

  The power source requirements are applicable to the plant design and are supported by the NUMAC platform. The ESBWR Safety I&C protection systems are supported by two independent safety-related 120 VAC power sources. Four divisions of redundant safety-related (uninterruptible) 120 VAC are used as the primary power source for the RTIF and NMS cabinets in which most components of the safety-related protection systems are located. Two divisions of the safety-related (uninterruptible) 120 VAC are

also used as the power sources for the solenoids of the scram pilot valves. Two divisions of the 250VDC power sources are used for the backup scram valve solenoids, for scram reset permissive logic.

4.2.8.17 Additional IEEE Std. 603 Compliance Discussion Applicable to RPS

In addition to the above general descriptions of compliance with IEEE Std. 603, a more specific discussion on compliance of IEEE Std. 603 by the RPS functions is included in this section.

- Safety System Criteria

  The RPS, including its logic, trip actuator logic, and trip actuators, is designed to comply with this requirement through automatic removal of electric power to the CRD scram pilot valve solenoids when a sufficient number of RPS variables exceed their specified trip setpoint.

- Single-Failure Criterion

  The RPS has four completely separate divisions with separate sensors whose only interaction is at the trip logic level via optical isolation. The system is in full compliance with the single-failure criterion and Regulatory Guide 1.53, with any three of the four divisions of safety-related power available.

- Quality

  All RPS components and modules and safety-related equipment of other systems providing inputs to the RPS are designed to maintain necessary functional capability under the extremes of conditions (as applicable) relating to environment, energy supply, malfunctions, and accidents, within which the equipment has been designed and qualified to operate continuously and without degradation.

- Equipment Qualification

  Instrument sensors and electrical components of the RPS and interfacing systems that are used for RPS functions are qualified for nuclear safety-related service for the function times and for the environment in which they are located. The RPS electrical safety-related equipment, including the RTIF controllers and cabinets, is qualified by type test, data from previous operating experience or analysis, or any combination of these three methods to substantiate that all equipment which must operate to provide the safety-related system actions will be capable of meeting, on a continuing basis, the necessary performance requirements.

- System Integrity

  RPS instrument channels, components, supporting equipment, and safety-related equipment of other systems providing inputs to the RPS are designed to maintain necessary functional capability under the extreme conditions relating to environment,

energy supply, malfunctions, and accidents, within which the equipment has been designed and qualified to operate continuously and without degradation.

- Channel Independence

  The RPS and supporting equipment are designed to assure that the effects of natural phenomena and of normal operation, maintenance, testing, and postulated accident conditions on redundant channels, divisions, and equipment of the RPS will not result in the loss of the safety function of the system.

  The redundant divisions of RPS are electrically and physically separated from each other such that (1) no design basis event is capable of damaging equipment in more than one division and (2) no single failure, test, calibration or maintenance operation can prevent the safety function of more than one division with any three of the four divisions of safety-related power available.

  Instrument channels that provide signals for the same protective function are independent and physically separated to accomplish the decoupling of the effects of unsafe environmental factors, electric transients, and physical accident consequences and to reduce the likelihood of interactions between channels during maintenance operations or in the event of channel malfunctions.

- Control and Protection System Interaction

  The channels for the RPS trip variables are electrically isolated and physically separated from the plant control systems in compliance with this design requirement.

  Multiple redundant sensors and channels assure that no single failure can prevent protective action with any three of the four divisions of safety-related power available.

- Derivation of System Inputs

  The following RPS trip variables are direct measures of a reactor overpressure condition, a reactor overpower condition, a reactor instability condition, a gross fuel damage condition, or abnormal conditions within the reactor coolant pressure boundary:

  - Reactor vessel low water level trip
  - NMS (APRM/OPRM) divisional trip
  - NMS (SRNM) divisional trip
  - Drywell high pressure trip
  - Reactor vessel high pressure trip
  - Other variables that could affect the RPS scram function itself and are monitored to induce a scram directly include:
    - Low charging pressure to control rod HCU accumulators
    - High suppression pool temperature

The detection of MSIV closure and turbine stop valve closure (if a sufficient number of bypass valves do not open in time) is an appropriate variable for the RPS. The desired variable is loss of the reactor heat sink; however, isolation (MSIV closure) or stop valve closure is the logical variable to indicate that the steam path has been blocked between the reactor and the heat sink.

Due to the normal throttling action of the turbine control valves with changes in the plant power level, measurement of control valve position is not an appropriate variable from which to infer the desired variable, which is rapid loss of the reactor heat sink. Consequently, a measurement related to control valve closure rate is necessary. Protection system design practice has discouraged the use of rate-sensing devices for protective purposes. In this instance, it was determined that detection of hydraulic actuator operation would be a more positive means of determining fast closure of the control valves. Loss of hydraulic pressure in the electro-hydraulic control (EHC) oil lines, which initiates fast closure of the control valves, is monitored. These measurements provide indication that fast closure of the control valves is imminent. This measurement is adequate and is a proper variable for the protective function, taking into consideration the reliability of the chosen sensors relative to other available sensors and the difficulty in making direct measurements of control valve fast-closure rate.

The Turbine Stop Valve closure and the steam governing Turbine Control Valve fast closure reactor scram is automatically bypassed when reactor power is below a preset setpoint value or if a sufficient number of the bypass valves are opening as indicated by their 10% position sensors.

- Capability for Test and Calibration

  The RPS fully meets this requirement in that it conforms with Regulatory Guides 1.22 and 1.118. The four-channel logic allows cross-checking between channels and the ability to take any one channel out of service during reactor operation. Such a condition is annunciated and automatically causes the channel trip logic to revert from two-out-of-four to two-out-of-three.

  Most sensors have a provision for actual testing and calibration during reactor operation. The exceptions are defined as follows:

  - During plant operation, the operator can confirm that the MSIV and turbine stop valve limit switches operate during valve motion. Precise calibration of these sensors requires reactor shutdown.
  - Independent functional testing of the air header dump valves can be performed during each refueling outage. In addition, operation of at least one valve can be confirmed following each scram occurrence.

- Operating Bypasses

  Whenever the applicable conditions for instrumentation scram bypasses are not met, the RPS will automatically accomplish one of the following: (1) prevent the actuation of an

operating bypass; (2) remove any active operating bypass; (3) obtain or retain the permissive conditions for the operating bypass; or (4) initiate the protective function.

- Indication of Bypasses

  Although operating bypasses do not require annunciation, certain operating bypasses are annunciated in the MCR. The CRD HCU accumulator low charging water pressure trip operating bypass, the MSIV closure trip operating bypass, the turbine stop and control valve fast closure trips operating bypass, and the division-of-sensors bypass are individually annunciated to the operator. Individual SRNM and APRM instrument channel bypasses are indicated on displays for each division on the MCR panels.

- Multiple Setpoints

  RPS trip variables are fixed except for the following, which are individually addressed.

  The trip setpoint of each SRNM channel is generally fixed. However, there is also the scram initiated by high neutron flux counting level (corresponding to nominally 5E + 5 counts per second). This is only activated in a non-coincidence scram mode by a switch in the NMS cabinet. The conditions under which such a trip is to be activated are included in plant operating procedures.

  In modes other than RUN, the APRM setdown function automatically selects a more restrictive scram trip setpoint at a fixed lower value (nominally at 15%). The devices used to prevent improper use of the less restrictive setpoints are designed in accordance with criteria regarding performance and reliability of protection system equipment.

  Operation of the mode switch from one position to another bypasses various RPS trips and channels and automatically alters NMS trip setpoints in accordance with the reactor conditions implied by the given position of the mode switch. Equipment associated with these setpoint changes are considered part of the protection system and qualified safety-related components.

- Completion of Protective Action

  It is only necessary that the process sensors remain in a tripped condition for a sufficient length of time to trip the digital trip modules and operate the seal-in circuitry, provided the two-out-of-four logic is satisfied. Once this action is accomplished, the trip actuator logic proceeds to initiate reactor scram regardless of the state of the process sensors that initiated the sequence of events. The same holds true for the manual scram pushbuttons.

- Manual Control

  Two manual scram pushbutton controls are provided on the principal MCR console to permit manual initiation of reactor scram at the system level. Both switches must be depressed to initiate a scram. Backup to these manual controls is provided by the SHUTDOWN position of the reactor system mode switch. Failure of the manual scram portion of the RPS cannot prevent the automatic initiation of protective action, nor can failure of an automatic RPS function prevent the manual portions of the system from initiating the protective action.

  No single failure in the manual or automatic portions of the system can prevent either a manual or automatic scram with any three of the four divisions of safety-related power available.

- Control of Access

  The RPS design permits the administrative control of access to all setpoint adjustments, module calibration adjustments and test points. These administrative controls are supported by provisions within the safety system design, by provisions in the generating station design, or by a combination of both.

- System Status Indication

  When any one of the redundant sensor trip modules exceeds its setpoint value for the RPS trip variables, a MCR display is initiated to identify the particular variable. In the case of NMS trips to the RPS, the specific variable or variables that exceed setpoint values are identified as a function of the NMS. Identification of the particular trip channel exceeding its setpoint is accomplished by permanent storage in the plant computer system. When any manual scram pushbutton is depressed, a MCR annunciation is initiated and a plant computer system record is produced to identify the tripped RPS trip logic.

- Repair

  Generally, all components can be replaced, repaired, and adjusted during operation. Exceptions are listed below.

  During periodic testing of the sensor channels for the following trip variables, defective components can be identified. Replacement and repair of failed sensors can only be accomplished during reactor shutdown.

  - NMS detectors
  - Turbine control valve fast closure sensors
  - MSIV closure sensors
  - Turbine stop valve closure sensors

Provisions have been made to facilitate repair of NMS components during plant operation except for the detectors. Replacement of the detectors can be accomplished only during shutdown.

- Identification

The RPS logic is housed in the RTIF cabinets. There are four distinct and separate cabinets in accordance with the four electrical divisions. Each division is uniquely identified by color code including cables and associated cables. The MCR panels are identified by tags on the panels, which indicate the function and identify the contained logic channels. Redundant racks are identified by the identification marker plates of instruments on the racks.

4.2.9 Testing and Inspection Requirements

- System Testing: Operational Verifiability

The NUMAC safety-related systems are designed with online self-test monitoring, and are designed so that individual operating elements can be periodically and independently tested to demonstrate that the NUMAC system is operable.

The NUMAC safety-related system design (and the design of other systems providing the safety-related system with instrument channel inputs) permits verification, with a high degree of confidence and during reactor operation, of the operational availability of each of the input sensors utilized by the NUMAC safety-related system (i.e., channel checks). In addition, the instrument channel inputs are continuously monitored by self-test.

The instrument channels are periodically calibrated and adjusted to verify that necessary precision and accuracy is being maintained. Such periodic checking and testing during plant operation is possible without loss of scram or trip capability and without causing an inadvertent scram or trip of a safety-related system.

The NUMAC safety-related system equipment is designed to allow inspection and testing during periodic shutdowns of the nuclear reactor and during refueling shutdowns.

- Surveillance Testing and In-Service Inspection

The NUMAC safety-related system equipment testing includes the following:

- Equipment qualification testing;
- Pre-operational, startup, and refueling/outage inspection testing; and
- In-service and operational surveillance testing.
- Continuous online self test diagnostics

The NUMAC safety-related systems are designed to permit testing of emergency reactor shutdown or system operations by methods simulating actual plant operation and duplicating, as closely as possible, the performance of protective actions, even during

reactor operation. These test methods support in-service verification of scram or trip capability with high reliability. To the extent practicable, the NUMAC safety-related system components and testing strategies are designed so that identifiable failures are detectable. Test methods are designed to facilitate recognition and location of malfunctioning components so that they may be replaced, adjusted, or repaired.

The NUMAC is designed to provide the capability for in-service testing of the NUMAC system channels to verify operability during normal plant operation and to assure that each tested channel can perform its intended design function. The surveillance tests include as required instrument channel checks, functional tests, verification of proper sensor and channel calibration, and response time tests in accordance with the established test procedures and as required by Technical Specifications.

Capability to perform logic functional tests and response time tests is provided; however, such testing is only supplementary to the online self-test diagnostics that continuously monitor and confirm that the software that implements the system logic and that was fully tested during the software V&V process has not inadvertently changed.

The system logic and response time requirements are provided as design inputs to the NUMAC design process. The equipment is designed and tested to meet these requirements. Logic that is contained in software does not need to be tested again once it has been validated and the software is monitored to confirm that it does not change. In the NUMAC system the vast majority of the system response time is attributable to digital filtering and logic that is performed in software. Any delays contributed by the hardware that performs the A/D conversion of the input signal and the solid-state hardware that provides the outputs to the scram solenoids and to the MSIV isolation solenoids is negligible by comparison. The response time of the NUMAC system does not need to be tested once the software has been validated and the software is monitored to confirm that it does not change. Periodic checks of the NUMAC system clock are performed to confirm that the clock is performing within specification.

4.3 EQUIPMENT QUALIFICATION

4.3.1 General

The qualification of the NUMAC instruments was established using qualification methods set forth in the General Electric Environmental Qualification Program (Reference 8-3). The NUMAC components have been qualified to operate in the normal and abnormal environments in which they are located. The environment includes temperature, humidity, pressure, seismic, radiation, and electro-magnetic interference (EMI).4.3.2 Environmental Qualification

4.3.2.1 Temperature and Humidity

4.3.2.1.1 General

The NUMAC components are qualified using type testing and analysis to demonstrate that they will perform all specified functions correctly when operated within the specified temperature range and relative humidity range.

4.3.2.1.2 Requirements

The NUMAC equipment is qualified in accordance with the following requirements:

- Reg. Guide 1.89
- IEEE Std. 323 - 2003

4.3.2.1.3 Compliance with Requirements

The NUMAC electronics are qualified in accordance with the above requirements for continuous operation under the design basis conditions of temperature and humidity for the installed location as defined in the DCD (Reference 8-6).

The NUMAC equipment is mounted in a mild environment, but the overall methodology used is the same as that used by GE for equipment located in a harsh (changes with the accident) environment. The qualification process includes a Product Analysis Report (PAR) that evaluates the design, compares it with previously completed qualification activities to identify similarities, and defines new qualification testing required. The evaluation assesses both replaceable modules and the overall assembly.

All qualification is based on type testing, either an assembly of the same design as the final product, or of an assembly that is sufficiently similar that an analysis can demonstrate equivalency for qualification purposes. Tests are performed in accordance with test plans and results are documented in test reports.

Qualification of modules includes measurement of all critical parameters to assure performance within module specifications over the full environmental range. Margins are included in accordance with the standards referenced above.

For the NUMAC instruments, some of the modules have previously been qualified, so the analysis need only show that the ESBWR application uses the modules within original qualified limits. Some modules were designed specifically for ESBWR so those are qualified for the first time for the NUMAC application. In either case, each separable module has its own performance specification and is qualified to a higher temperature than the chassis into which it is installed to allow for internal (to the chassis) temperature rise.

Chassis qualification includes modules, but measurements are made to ensure performance within chassis specifications. That is, only the module functions required for the application are checked during chassis testing.

4.3.2.2 Pressure

4.3.2.2.1 General

The NUMAC instrument is qualified by analysis to perform to specification for any absolute pressure in the range specified.

4.3.2.2.2 Requirements

The specific requirements for qualification for the pressure conditions during normal and accident conditions are defined in the DCD (Reference 8-6).

4.3.2.2.3 Compliance with Requirements

The NUMAC electronics are qualified for continuous operation under the design basis pressure conditions for the installed location of the equipment as defined in the DCD (Reference 8-6).

The qualification for pressure is performed by analysis of the components.

4.3.2.3 Radiation

4.3.2.3.1 General

The NUMAC electronics are qualified by analysis to perform within specification limits over their service life under the specified radiation conditions.

4.3.2.3.2 Requirements

The specific requirements for qualification for the radiation conditions during normal and accident conditions are defined in the DCD (Reference 8-6).

4.3.2.3.3 Compliance with Requirements

The NUMAC electronics are qualified for continuous operation under the following conditions:

- Dose Rate: 1 E-3 Rads (gamma)/hr or less
- Total Integrated Dose (TID): 1 E+3 Rads (gamma)

The above conditions apply at the hardware mounting location.

Due to the low levels of radiation, qualification is performed by analysis of the specific components to confirm that radiation levels defined above will not affect performance. The basis of analysis is industry data on the specific or similar components.

4.3.3 Seismic Qualification

4.3.3.1 General

The NUMAC electronics are qualified by type testing and analysis to demonstrate that the NUMAC instrument will perform all specified functions correctly when operated within the specified seismic limits and when mounted in accordance with the specified mounting methods.

4.3.3.2 Requirements

The NUMAC electronics are qualified in accordance with the following requirements:

- Reg Guide 1.100 (IEEE Std. 344 - 1975)

4.3.3.3 Compliance with Requirements

The NUMAC electronics are qualified to operate (or provide a trip) through a seismic event not exceeding the limits defined for the specific location of installation, using the guidance provided in the requirements above. The specific requirements for qualification for the seismic conditions are defined in the DCD (Reference 8-6).

Qualification is based on type testing performed with equipment mounted in accordance with the requirements of applicable interface control documents, which are also used to define mounting requirements for the installed equipment. Testing is performed in accordance with test procedures based on the requirements of the above standards, including applicable margins. Performance is monitored for all critical functions for the equipment before, during, and after the seismic tests. Results are documented in test reports.

4.3.4 EMI Qualification

4.3.4.1 EMI General

The NUMAC components, when mounted in accordance with the specified mounting methods, are qualified by type testing and analysis to demonstrate that they will perform all specified functions correctly when operated within the specified EMI limits.

The NUMAC equipment is not susceptible to electromagnetic disturbances from neighboring modules and does not cause electromagnetic disturbances to neighboring modules.

4.3.4.2 Requirements

The NUMAC instrument is qualified in accordance with the following requirements:

- Reg Guide 1.180, Rev 1
- EPRI TR-102323

4.3.4.3 Compliance with Requirements

The NUMAC equipment is qualified, using methods defined in the requirements above, to perform within its specifications continuously while exposed to EMI environmental limits defined in the requirements. The NUMAC equipment will not emit EMI exceeding the limits defined in the requirements when measured using the methods defined, as applicable. The above conditions apply at the hardware mounting location, and envelope the limits defined in EPRI Report TR-102323 (Reference 8-4).

The EMI susceptibility and emissions testing is performed by type testing using a representative "system" comprising all of the NUMAC system and sub-assemblies, interconnecting cables, and fluorescent fixtures and switches typically found in a panel. The equipment is mounted in a steel panel representative of the actual field mounting. Testing is done with panel doors open to cover maintenance conditions and a few cases that do not use doors. Applications using doors will have additional margin during normal operating condition (doors closed). All critical functions are monitored during the testing to assure that no abnormal operation occurs as a result of EMI.

In addition to the above qualification, the ESBWR design includes grounding methods, cabling separation to assure that signal cables with the potential to be "receivers" are kept separate from cables that are sources of noise, and equipment separation and shielding practices that are effective in minimizing the EMI effects, both relative to susceptibility and emissions.

5.0 SYSTEM AND EQUIPMENT DESCRIPTION

5.1 RTIF SYSTEM

5.1.1 RTIF System Description

5.1.1.1 General

The Reactor Trip and Isolation Function (RTIF) performs the Reactor Protection System (RPS) functions, the Main Steam Isolation Valve (MSIV) closure functions, and the Suppression Pool Temperature Monitoring (SPTM) function for the ESBWR. The system also provides bypass handling, surveillance, and self-test functions. For RPS, RTIF provides the RPS scram signal. For MSIV, RTIF provides the MSIV isolation signal. These trip signals are based on sensor inputs, pre-determined setpoints, and exclusionary bypass and voting logic. The RTIF also provides the necessary data to external systems via the safety-related Q-DCIS and nonsafety-related N-DCIS systems. The RTIF consists of four safety-related divisions, each operating independently. A failure in one division with any three of the four divisions of safety-related power available will not adversely impact the safety function of the system.

Each safety division of RTIF comprises the following:

- Remote Multiplexing Unit (RMU)
- Digital Trip Module (DTM)
- Trip Logic Unit (TLU)
- Communication Interface Module (CIM)
- RPS Output Logic Unit (RPS OLU)
- MSIV Output Logic Unit (MSIV OLU)
- RPS Load Drivers (RPS LD) (Div 1 and Div 2 only)
- MSIV Load Drivers (MSIV LD) (Div 1 and Div 2 only)
- Bypass Unit (BPU)
- Local Display Unit (LDU)

The instruments in each RTIF division operate collectively to accomplish the safety-related functions for the RPS and MSIV. While the instruments within a division work together and share data, they operate independently of each other so that a failure in one instrument will not affect the operation of another. A description of each of the instruments is provided in the following sub-sections.

5.1.1.2 Equipment Safety Classification

The RTIF is classified as a safety-related system, but not all components within the RTIF perform safety-related functions. The RTIF LDU is classified as nonsafety-related because it does not perform any safety-related functions.

5.1.1.3 Components Required to Perform Safety Functions

The major components of the RTIF that must function at least in part to perform the system safety-related functions are the following:

- RMU Chassis
- DTM Chassis
- TLU Chassis
- CIM Chassis
- RPS OLU and MSIV OLU Chassis
- RPS LD and MSIV LD Chassis
- BPU Chassis
- Quad Low Voltage Power Supplies

Portions of the above components are not required to operate to accomplish the system safety-related function, but they must maintain physical integrity under all conditions and must not cause any fault that can disable power to the components required to perform safety-related functions except in a fail safe mode (loss of power), or cause a fault that affects the UPS power supplies to the RTIF panels except in a fail safe mode (loss of power).

These components are classified safety-related.

5.1.1.4 Components Required to Not Fail Detrimentally

The following major component is not required to operate to accomplish the system safety-related functions, but it must maintain physical integrity under all conditions.

- LDU

All interfaces between the LDU and equipment performing system safety-related functions are via fiber optic cable.

5.1.1.5 Components Purchased Commercial and Dedicated

The Low Voltage Power Supply (LVPS) modules are purchased to GE drawing numbers and specifications. The LVPS Modules are dedicated and re-identified according to the test procedures and acceptance criteria specified in the applicable GE drawings and specifications.

The same LVPS module is used for all NUMAC instruments, including the RTIF. The dedication process for the modules is the same regardless of the final application.

The dedication process is similar to that defined in EPRI Report No. NP-5652 (Reference 8-13), but is actually controlled by the GE Engineering Operating Procedures. Per those procedures, the dedication process includes both a "design" phase and a "production" phase.

During the design phase, the target product is defined or identified. In the case of the LVPS, specific required technical specifications were defined. The vendors then adapted their standard products to a design that met the GE requirements. In conjunction with this process, one of the following qualification methods is selected:

- One time qualification of the design, via type testing of pilot units, to be followed by actions to confirm that each delivered item conforms to the design originally qualified, or
- Lot production batch qualification, performed for each production lot, with confirmation that each member of the lot is identical.

For the LVPS, vendor quality surveys of the intended supplier confirmed that they had in place quality programs of sufficient strength that confirmation of design similarity could be determined, so the first method (one time qualification) was selected.

The process also calls for identification of critical characteristics and establishing a production receiving process of inspections and tests to assure that each LVPS met the required critical characteristics. The combination of successful passage of the receiving requirements along with periodic quality reviews of the suppliers to assure that no significant design changes occurred provides the basis of dedication for the actual production modules.

5.1.2 Functions of Major System Level Hardware

5.1.2.1 Remote Multiplexing Unit (RMU)

There are four RMU channels in the RTIF System, one in each division, located in the reactor building. All RMU chassis, regardless of channel assignment, are identical and fully interchangeable. Each RMU chassis automatically configures itself for the particular RMU channel when the chassis is powered up. The RMU chassis determines the channel identification by examination of identification jumpers provided at each RMU chassis location as part of the panel wiring, which is unique to each division.

The primary purpose of the RMU is to digitize sensor signals that are acquired in the reactor building and to transmit the data to the DTM for use in trip calculations. The RMU calculates the suppression pool bulk average temperature and provides this data to the DTM as well.

5.1.2.2 Digital Trip Module (DTM)

There are four DTM channels in the RTIF System, one in each division, located in the control building. All DTM chassis, regardless of channel assignment, are identical and fully

interchangeable. Each DTM chassis automatically configures itself for the particular DTM channel when the chassis is powered up. The DTM chassis determines the channel identification by examination of identification jumpers provided at each DTM chassis location as part of the panel wiring, which is unique to each division.

The primary purpose of the DTM is to digitize sensor signals that are acquired in the control building that originate in both the control building and in the turbine building, perform engineering units conversion on these signals, perform engineering units conversion on raw data acquired by the RMU in the reactor building, and use the resulting values in performing divisional RPS scram and MSIV isolation trip calculations. The DTM produces trip signals (trip/no trip) that are output to the TLU in each of the four divisions.

5.1.2.3 Trip Logic Unit (TLU)

There are four TLU channels in the RTIF System, one in each division, located in the control building. All TLU chassis, regardless of channel assignment, are identical and fully interchangeable. Each TLU chassis automatically configures itself for the particular TLU channel when the chassis is powered up. The TLU chassis determines the channel identification by examination of identification jumpers provided at each TLU chassis location as part of the panel wiring, which is unique to each division.

The primary purpose of the TLU is to receive and process trip input signals from the DTM in each of the four divisions, perform two-out-of-four voting on the DTM channel trip signals to produce divisional trip signals, output a trip command to the RPS OLU when a divisional RPS scram trip condition exists, and output a trip command to the MSIV OLU when a divisional MSIV isolation trip condition exists. The TLU also processes the trip inputs from the NMS.

5.1.2.4 Communication Interface Module (CIM)

There are four CIM channels in the RTIF System, one in each division, located in the control building. All CIM chassis, regardless of channel assignment, are identical and fully interchangeable. Each CIM chassis automatically configures itself for the particular CIM channel when the chassis is powered up. The CIM chassis determines the channel identification by examination of identification jumpers provided at each CIM chassis location as part of the panel wiring, which is unique in each division.

The primary purpose of the CIM is to receive data messages from the other instruments in the RTIF division and transmit this data to other systems as required by external protocols. The CIM is the gateway to the N-DCIS and Q-DCIS systems for the rest of the RTIF instruments in the division.

5.1.2.5 RPS Output Logic Unit (RPS OLU)

The NUMAC RPS OLU is a non-microprocessor based component in the RTIF system. The RPS OLU is designed to perform the following:

- Receive signals from the TLU and initiate Auto RPS Scram (de-energization of the RPS Load Drivers).
- Receive signals from the TLU and initiate a trip of the Backup Scram.
- Transmit OLU status to the CIM.

The RTIF uses four RPS OLU instruments, one per safety division. Each instrument is identically configured and contains the entire configuration variations required for any of the RTIF divisions. Configuration is done by external jumpers on the back panel connectors.

The RPS OLU contains a microcontroller with firmware that implements the self-test function and controls the status indication devices on the front panel. These functions are isolated from the RPS OLU logic in such a way that any firmware fault does not impair the safety-related function of the RPS OLU.

5.1.2.6 MSIV Output Logic Unit (MSIV OLU)

The NUMAC MSIV OLU is a non-microprocessor based component in the RTIF system. The MSIV OLU is designed to perform the following:

- Receive signals from the TLU and initiates Auto Isolation (de-energization of the MSIV Load Drivers)
- Transmit status to the CIM.

The RTIF uses four MSIV OLU instruments, one per safety division. Each instrument is identically configured and contains the entire configuration variations required for any of the RTIF divisions. Configuration is done by external jumpers on the back panel connectors.

The MSIV OLU contains a microcontroller with firmware that implements the self-test function and controls the status indication devices on the front panel. These functions are isolated from the MSIV OLU logic in such a way that any firmware fault does not impair the safety-related function of the MSIV OLU.

5.1.2.7 Load Driver (LD)

The basic LD module contains four individual solid-state switches that are capable of switching 120 VAC electrical power to banks of solenoids. Each switch is connected to a controlling Output Logic Unit (OLU) by a single fiber optic cable that provides a full duplex communication channel, which means that the switch receives commands from, and transmits self-test information back to, the OLU through a single cable. The fiber optic cable also provides electrical isolation that facilitates communication across division boundaries without additional isolation devices.

The LD module switch logic is hardwired, i.e. switches are arranged in series and in parallel in order to accomplish the desired logic function. The functionality of each individual switch is implemented in hardware only.

The LD module contains a microcontroller with firmware that implements the self-test function and controls the status indication devices on the front panel. These functions are isolated from the LD logic in such a way that any firmware fault does not impair the safety-related function of the LD module.

5.1.2.8 Bypass Unit (BPU)

The RTIF Bypass unit is designed to send four separate groups of bypass signals, each initiated through a Fiber Optic Bypass Switch. The bypass signals are identified as Division of Sensors Bypass, Division of Logic Bypass (Division-Out-Of-Service Bypass), Special Isolated Main Steam Line Operational Bypass, and ATWS Logic Output Bypass. The Division of Sensors Bypass and Special Isolated Main Steam Line Operational Bypass are used by the TLU. The Division of Logic Bypass is used by the RPS OLU and the MSIV OLU.

The RTIF uses four RTIF Bypass Units, one instrument for each safety division and each instrument is identically configured.

5.1.2.9 Local Display Unit (LDU)

The RTIF Local Display Unit (LDU) is a "stand-alone" microprocessor-based system designed to provide a user interface with the RMU, DTM, TLU, and CIM instruments.

The purpose of the RTIF LDU is to allow the user to view system data, maintain database parameters, meet surveillance requirements, perform calibrations where applicable, and run diagnostic programs at the connected RTIF equipment. Predefined displays for the RTIF equipment within the LDU include:

- System Data Displays for monitoring instrument operating data, instrument hardware configuration status, and I/O channel operational status.
- Database Parameter Displays for the modification of predefined parameter data in non-volatile memory.
- Self-Test Menu Displays for diagnostic program selection to test both the physical configuration and each type of I/O channel including the discrete I/O channels and data link channels.
- Calibration and Calibration Check displays.
- Trip Check and Output Check displays.

5.1.3 RTIF Communication Interfaces

5.1.3.1 RTIF Replicated Memory Networks

5.1.3.1.1 General

A replicated memory network is a shared memory interface that allows each node on the network to read and write from the same virtual memory space. A single replicated memory network interface module installed in a NUMAC instrument represents a single network node. Data is exchanged between the NUMAC microprocessor and the replicated memory network interface module over the NUMAC data bus via a dual port RAM interface on the replicated memory network interface module. Each replicated memory network interface module is assigned a unique base address such that memory read/write operations are restricted to a single network node. A replicated memory network comprises multiple network nodes connected via fiber optic ring architecture.

Dual counter-rotating network rings provide a redundant network architecture that is extremely fault tolerant. Two network nodes in each instrument, a primary and a secondary, are required to implement the dual counter-rotating replicated memory network architecture. Multiple dual counter-rotating replicated memory networks are used in the RTIF system to maintain separation between safety-related and nonsafety-related functions.

5.1.3.1.2 Safety-Related Divisional Ring Network

The RTIF safety-related divisional ring network is a dual counter-rotating replicated memory network that connects the RMU, DTM, TLU, and CIM instruments within a single RTIF division. This network provides the data highway for safety-related data to be shared between the RTIF instruments in the division and to make this data available to external systems via the CIM instrument. The CIM is the gateway between the safety-related divisional ring network and other systems.

5.1.3.1.3 Nonsafety-Related Common Ring Network

The nonsafety-related common ring network is a dual counter-rotating replicated memory network that is used by multiple nonsafety-related systems and provides the gateway to the nonsafety-related displays in the MCR and other N-DCIS systems. The CIM in each division interfaces with the nonsafety-related common ring network. The CIM provides a buffer function between the safety-related RTIF and other nonsafety-related systems.

5.1.3.1.4 Nonsafety-Related LDU Network – Control Building

This nonsafety-related LDU network is a dual counter-rotating replicated memory network that connects the DTM, TLU, and CIM instruments within a single RTIF division with the nonsafety-related LDU user interface located in the RTIF panel. The transfer of data across this network is

normally one-way, from the RTIF instruments to the LDU, to facilitate local display of data and status information. A keylock switch on the DTM, TLU, and CIM instruments may be used to place an instrument in the Inoperative Mode that allows for two-way communication between the instrument and the LDU to facilitate setup of instrument parameters, calibration of the electronics, and performance of certain diagnostic functions.

5.1.3.1.5 Nonsafety-Related LDU Network – Reactor Building

This nonsafety-related LDU network is a dual counter-rotating replicated memory network that connects the RTIF RMU in the reactor building with the nonsafety-related LDU user interface located in the RTIF RMU panel. The transfer of data across this network is normally one-way, from the RMU to the LDU, to facilitate local display of data and status information. A keylock switch on the RMU instrument may be used to place the instrument in the Inoperative Mode that allows for two-way communication between the RMU and the LDU to facilitate setup of instrument parameters, calibration of the electronics, and performance of certain diagnostic functions.

5.1.3.2 RTIF Inter-Divisional Trip Signals

Inter-divisional communication of channel trip status to facilitate two-out-of-four voting of the RPS channel trips is provided by MIL-STD-1553 point-to-point fiber optic communication links between the DTM and TLU instruments in the RTIF system. The DTM provides four dynamic fiber optic trip status outputs, one output for each of the four TLU instruments. The TLU provides four fiber optic inputs, one input for each of the four DTM instruments. The RTIF Division of Sensors bypass may be used to bypass the RPS trip inputs from one of the four DTM channels.

The trip signal must be continuously refreshed in order to remain valid. The protocol provides for parity and Manchester II encoding checks to confirm the integrity of the trip signal. If the signal is not properly refreshed or is determined to be invalid, the system defaults to a tripped state for the failed input.

5.1.3.3 N-DCIS

5.1.3.3.1 General

The CIM provides a gateway between RTIF and the nonsafety-related common ring network. There is no direct path between the RTIF safety-related divisional ring network and the nonsafety-related common ring network, and all data transfers are processed by the CIM as memory read/write operations from/to the dual port RAM interface on the associated replicated memory network interface modules.

5.1.3.3.2 Safety-Related System to Nonsafety-Related System Communications

Data from the RTIF instruments (RMU, DTM, TLU) is provided to the CIM over the safety-related divisional ring network. The CIM transfers data from the safety-related divisional ring network to the nonsafety-related common ring network for use by the nonsafety-related systems on the nonsafety-related common ring network. The common ring network also provides gateways for the purpose of transmitting RTIF data to the nonsafety-related VDUs in the MCR and other nonsafety-related N-DCIS systems.

5.1.3.3.3 Nonsafety-Related System to Safety-Related System Communications

The CIM provides a buffer function for data transmitted from the nonsafety-related common ring network to RTIF. The only data transmitted from the nonsafety-related common ring network to RTIF is a time-of-day signal used for local display and time-tagging of data. The time-of-day signal is periodically transmitted from the nonsafety-related common ring network to the RTIF CIM. When the processing of safety-related functions allows, the CIM reads the data from the dual port RAM of the replicated memory network interface associated with the nonsafety-related common ring network, performs data validation checks, and if found to be valid writes the data to the replicated memory network interface associated with the safety-related divisional ring network, where the data can be accessed by the other RTIF instruments.

5.1.3.4 Q-DCIS

The RTIF CIM provides dedicated redundant fiber optic serial data outputs to the Q-DCIS for the purpose of transmitting RTIF data to the safety-related VDUs in the MCR and to other safety-related systems. The communication is one-way, from the RTIF CIM to the Q-DCIS.

5.1.3.5 Communications with NMS

The RTIF TLU maintains a bidirectional fiber optic communication link with the NMS TLU in the same division. The protocol has the same dynamic signal characteristics as that used for the inter-divisional trip signals. The RTIF TLU transmits reactor mode status to the NMS TLU over this link, and receives the SRNM and PRNM trip outputs from the NMS TLU over this link.

5.2 NMS SYSTEM

5.2.1 NMS System Description

5.2.1.1 General

The NMS portion of the Reactor Trip System includes the SRNM and PRNM sub-systems of the NMS. The NMS consists of four safety divisions, each operating independently. A failure in one division with any three of the four divisions of safety-related power available will not adversely affect the safety-related function of the system.

Each safety division of NMS comprises the following:

- SRNM Preamplifier (one per channel)
- SRNM Remote Multiplexing Unit (SRNM RMU)
- PRNM Remote Multiplexing Unit (PRNM RMU)
- Digital Trip Module (DTM)
- Trip Logic Unit (TLU)
- Communication Interface Module (CIM)
- Bypass Unit (BPU)
- Local Display Unit (LDU)

The instruments in each NMS division operate collectively to accomplish the safety functions for the SRNM and PRNM sub-systems. While the instruments within a division work together and share data, they operate independently of each other so that a failure in one instrument will not impact the operation of another. A description of each of the instruments is provided in sections below.

5.2.1.2 Equipment Safety Classification

While the NMS is classified as a safety-related system, not all components within the NMS perform safety-related functions. The NMS LDU is classified as nonsafety-related because it does not perform safety-related functions.

5.2.1.3 Components Required to Perform Safety Functions

The major components of the NMS that must function at least in part to perform the system safety-related functions are the following:

- SRNM Preamplifier
- SRNM RMU chassis
- PRNM RMU chassis
- DTM chassis
- TLU Chassis
- CIM Chassis
- BPU Chassis

Portions of the above components are not required to operate to accomplish the system safety-related functions, but they must maintain physical integrity under all conditions and must not cause any fault that can disable power to the components required to perform safety-related

functions except in a fail safe mode (loss of power), or cause a fault that affects the UPS power supplies to the NMS panels except in a fail safe mode (loss of power).

These components are classified safety-related.

5.2.1.4 Components Required to Not Fail Detrimentally

The following major component is not required to operate to accomplish the system safety-related functions, but it must maintain physical integrity under all conditions.

- Local Display Unit

All interfaces between the LDU and equipment performing system safety-related functions are via fiber optic cable.

5.2.1.5 Components Purchased Commercial and Dedicated

The Low Voltage Power Supply (LVPS) and High Voltage Power Supply (HVPS) modules are purchased to GE drawing numbers and specifications. The LVPS and HVPS Modules are dedicated and re-identified according to the test procedures and acceptance criteria specified in the applicable GE drawings and specifications. The same LVPS module is used for all NUMAC instruments, including the NMS. The dedication process for the modules is the same regardless of the final application.

The dedication process is similar to that defined in EPRI Report No. NP5652 (Reference 8-13), but is actually controlled by the GE Engineering Operating Procedures. Per those procedures, the dedication process includes both a "design" phase and a "production" phase.

During the design phase, the target product is defined or identified. In the case of the LVPS and HVPS, specific required technical specifications were defined. The vendors then adapted their standard products to a design that met the GE requirements. In conjunction with this process, one of the following qualification methods is selected:

- One time qualification of the design, via type testing of pilot units, to be followed by actions to confirm that each delivered item conforms to the design originally qualified, or
- Lot production batch qualification, performed for each production lot, with confirmation that each member of the lot is identical.

For the LVPS and HVPS, vendor quality surveys of the intended supplier confirmed that they had in place quality programs of sufficient strength that confirmation of design similarity could be determined, so the first method (one time qualification) was selected.

The process also calls for identification of critical characteristics and establishing a production receiving process of inspections and tests to assure that each LVPS and HVPS met the required critical characteristics. The combination of successful passage of the receiving requirements along with periodic quality reviews of the suppliers to assure that no significant design changes occurred provides the basis of dedication for the actual production modules.

5.2.2 Functions of Major System Level Hardware

5.2.2.1 SRNM Preamplifier

The SRNM preamplifier amplifies the signal received from a neutron sensor and transmits a single output to the associated SRNM RMU chassis. The preamplifier covers the entire range for the SRNM operation, providing amplification from pulse signals to MSV range signals. There are twelve SRNM preamplifiers in the NMS, three in each division, located in the reactor building.

5.2.2.2 SRNM Remote Multiplexing Unit (SRNM RMU)

There are twelve SRNM RMU channels in the NMS, three in each division, located in the reactor building. All SRNM RMU chassis, regardless of channel assignment, are identical and fully interchangeable.

The primary function of the SRNM RMU is to monitor the associated SRNM detector, calculate the SRNM channel power and period, and transmit this data to the NMS DTM for use in SRNM trip and alarm calculations.

5.2.2.3 PRNM Remote Multiplexing Unit (PRNM RMU)

There are four PRNM RMU channels in the NMS, one in each division, located in the reactor building. Each PRNM RMU channel consists of two PRNM RMU chassis, a master and a slave. All master PRNM RMU chassis, regardless of channel assignment, are identical and fully interchangeable. All slave PRNM RMU chassis, regardless of channel assignment, are identical and fully interchangeable. Each PRNM RMU chassis automatically configures itself for the particular PRNM RMU channel when the chassis is powered up. The PRNM RMU chassis determines the channel identification by examination of identification jumpers provided at each RMU chassis location as part of the panel wiring, which is unique to each division.

LPRM inputs for the division are distributed between the master and the slave. The slave provides its LPRM data to the master for further processing. The master uses all LPRM data from both chassis to calculate the APRM flux, APRM simulated thermal power, and to perform stability monitor calculations. The LPRM, APRM, and OPRM data are then transmitted to the DTM for use in PRNM trip and alarm calculations.

5.2.2.4 Digital Trip Module (DTM)

There are four DTM channels in the NMS, one in each division, located in the control building. All DTM chassis, regardless of channel assignment, are identical and fully interchangeable. Each DTM chassis automatically configures itself for the particular DTM channel when the chassis is powered up. The DTM chassis determines the channel identification by examination of identification jumpers provided at each DTM chassis location as part of the panel wiring, which is unique to each division.

The primary purpose of the DTM is to perform all SRNM and PRNM trip and alarm calculations. The DTM produces trip signals (trip/no trip) that are output to the TLU in each of the four divisions.

5.2.2.5 Trip Logic Unit (TLU)

There are four TLU channels in the NMS, one in each division, located in the control building. All TLU chassis, regardless of channel assignment, are identical and fully interchangeable. Each TLU chassis automatically configures itself for the particular TLU channel when the chassis is powered up. The TLU chassis determines the channel identification by examination of identification jumpers provided at each TLU chassis location as part of the panel wiring, which is unique to each division.

The primary purpose of the TLU is to receive and process trip input signals from the DTM in each of the four divisions, perform two-out-of-four voting on the DTM channel trip signals to produce divisional trip signals, and output the SRNM and PRNM trip status to RTIF. The TLU receives SRNM and APRM bypass status from each of the four divisions. The TLU also provides ADS Inhibit and ATWS Permissive outputs.

5.2.2.6 Communication Interface Module (CIM)

There are four CIM channels in the NMS, one in each division, located in the control building. All CIM chassis, regardless of channel assignment, are identical and fully interchangeable. Each CIM chassis automatically configures itself for the particular CIM channel when the chassis is powered up. The CIM chassis determines the channel identification by examination of identification jumpers provided at each CIM chassis location as part of the panel wiring, which is unique to each division.

The primary purpose of the CIM is to receive data messages from the other instruments in the NMS division and transmit this data to other systems as required by external protocols. The CIM is the gateway to the N-DCIS and Q-DCIS systems for the rest of the NMS instruments in the division.

5.2.2.7 Bypass Unit (BPU)

The NMS Bypass unit is designed to send four separate groups of bypass signals that are associated with the three SRNM channels and the APRM channel in the division, each initiated through separate Fiber Optic Bypass Switches. The bypass signals in each Division are identified as SRNM Channel 1 Bypass, SRNM Channel 2 Bypass, SRNM Channel 3 Bypass, and APRM Bypass. In addition, the NMS Bypass Unit generates a divisional SRNM Bypass signal when all three channels in the division are bypassed at the same time. The SRNM Channel 1 Bypass, SRNM Channel 2 Bypass, and SRNM Channel 3 Bypass signals are used by the DTM. The divisional SRNM Bypass and APRM Bypass are used by the TLU.

The NMS uses four NMS Bypass Units, one instrument for each safety division, and each instrument is identically configured.

5.2.2.8 Local Display Unit (LDU)

The NMS Local Display Unit (LDU) is a "stand-alone" microprocessor-based system designed to provide a user interface with the SRNM RMU, PRNM RMU, DTM, TLU, and CIM instruments.

The purpose of the NMS LDU is to allow the user to view system data, maintain database parameters, meet surveillance requirements, perform calibrations where applicable, and run diagnostic programs at the connected NMS equipment. Predefined displays for the NMS equipment within the LDU include:

- System Data Displays for monitoring instrument operating data, instrument hardware configuration status, and I/O channel operational status.
- Database Parameter Displays for the modification of predefined parameter data in non-volatile memory.
- Self-Test Menu Displays for diagnostic program selection to test both the physical configuration and each type of I/O channel including the discrete I/O channels and data link channels.
- Calibration and Calibration Check displays.
- Trip Check and Output Check displays.

5.2.3 NMS Communication Interfaces

5.2.3.1 NMS Replicated Memory Networks

5.2.3.1.1 General

A replicated memory network is a shared memory interface that allows each node on the network to read and write from the same virtual memory space. A single replicated memory network

interface module installed in a NUMAC instrument represents a single network node. Data is exchanged between the NUMAC microprocessor and the replicated memory network interface module over the NUMAC data bus via a dual port RAM interface on the replicated memory network interface module. Each replicated memory network interface module is assigned a unique base address such that memory read/write operations are restricted to a single network node. A replicated memory network comprises multiple network nodes connected via fiber optic ring architecture.

Dual counter-rotating network rings provide a redundant network architecture that is extremely fault tolerant. Two network nodes in each instrument, a primary and a secondary, are required to implement the dual counter-rotating replicated memory network architecture. Multiple dual counter-rotating replicated memory networks are used in the NMS to maintain separation between safety-related and nonsafety-related functions.

5.2.3.1.2 Safety-Related Divisional Ring Network

The NMS safety-related divisional ring network is a dual counter-rotating replicated memory network that connects the SRNM RMU, PRNM RMU, DTM, TLU, and CIM instruments within a single NMS division. This network provides the data highway for safety-related data to be shared between the NMS instruments in the division and to make this data available to external systems via the CIM instrument. The CIM is the gateway between the safety-related divisional ring network and other systems.

5.2.3.1.3 Nonsafety-Related Common Ring Network

The nonsafety-related common ring network is a dual counter-rotating replicated memory network that is used by multiple nonsafety-related systems and provides the gateway to the nonsafety-related displays in the MCR and other N-DCIS systems. The CIM in each division interfaces with the nonsafety-related common ring network. The CIM provides a buffer function between the safety-related NMS and other nonsafety-related systems.

5.2.3.1.4 Nonsafety-Related LDU Network – Control Building

This nonsafety-related LDU network is a dual counter-rotating replicated memory network that connects the DTM, TLU, and CIM instruments within a single NMS division with the nonsafety-related LDU user interface located in the RTIF panel. The transfer of data across this network is normally one-way, from the NMS instruments to the LDU, to facilitate local display of data and status information. A keylock switch on the DTM, TLU, and CIM instruments may be used to place an instrument in the Inoperative Mode that allows for two-way communication between the instrument and the LDU to facilitate setup of instrument parameters, calibration of the electronics, and performance of certain diagnostic functions.

5.2.3.1.5 Nonsafety-Related LDU Network – Reactor Building

This nonsafety-related LDU network is a dual counter-rotating replicated memory network that connects the SRNM RMU and PRNM RMU in the reactor building with the nonsafety-related LDU user interface located in the NMS RMU panel. The transfer of data across this network is normally one-way, from the SRNM RMU and PRNM RMU to the LDU, to facilitate local display of data and status information. A keylock switch on the SRNM RMU and PRNM RMU instruments may be used to place an instrument in the Inoperative Mode that allows for two-way communication between the instrument and the LDU to facilitate setup of instrument parameters, calibration of the electronics, and performance of certain diagnostic functions.

5.2.3.2 NMS Inter-Divisional Trip Signals

Inter-divisional communication of channel trip status to facilitate two-out-of-four voting of the SRNM and PRNM channel trips is provided by MIL-STD-1553 point-to-point fiber optic communication links between the DTM and TLU instruments in the NMS. The DTM provides four dynamic fiber optic trip status outputs, one output for each of the four TLU instruments. The TLU provides four fiber optic inputs, one input for each of the four DTM instruments. The SRNM trip inputs from one of the four DTM channels may be bypassed by placing all of the SRNM channels in the division in bypass. The PRNM trip inputs from one of the four DTM channels may be bypassed by placing the APRM channel in bypass.

The trip signal must be continuously refreshed in order to remain valid. The protocol provides for parity and Manchester II encoding checks to confirm the integrity of the trip signal. If the signal is not properly refreshed or is determined to be invalid, the system defaults to a tripped state for the failed input.

5.2.3.3 N-DCIS

5.2.3.3.1 General

The CIM provides a gateway between NMS and the nonsafety-related common ring network. There is no direct path between the NMS safety-related divisional ring network and the nonsafety-related common ring network, and all data transfers are processed by the CIM as memory read/write operations from/to the dual port RAM interface on the associated replicated memory network interface modules.

5.2.3.3.2 Safety-Related System to Nonsafety-Related System Communications

Data from the NMS instruments (SRNM RMU, PRNM RMU, DTM, TLU) is provided to the CIM over the safety-related divisional ring network. The CIM transfers data from the safety-related divisional ring network to the nonsafety-related common ring network for use by the nonsafety-related systems on the nonsafety-related common ring network. The common ring network also provides gateways for the purpose of transmitting NMS data to the nonsafety-related VDUs in the MCR and other nonsafety-related N-DCIS systems.

5.2.3.3.3 Nonsafety-Related System to Safety-Related System Communications

The CIM provides a buffer function for data transmitted from the nonsafety-related common ring network to NMS. The only data transmitted from the nonsafety-related common ring network to NMS is a time-of-day signal used for local display and time-tagging of data, as well as LPRM and APRM calibration gain adjustment factors. The NMS CIM processes the time-of-day signal in exactly the same manner as the RTIF CIM (see Section 5.1.3.3.3). The LPRM and APRM calibration gain adjustment factors are transmitted on demand, initiated by the operator under administrative control. When the processing of safety-related functions allows, the CIM reads the LPRM and APRM gain adjustment factors from the dual port RAM of the replicated memory network interface associated with the nonsafety-related common ring network, performs data validation checks, and if found to be valid writes the data to the replicated memory network interface associated with the safety-related divisional ring network, where the gain adjustment factors can be accessed by the PRNM RMU instruments. A keylock switch is used to place the PRNM in Inoperative Mode before the gain adjustment factors can be applied, and the pending gain values must be manually accepted by the operator. Once accepted, the gain values are stored in non-volatile memory and applied to subsequent LPRM and APRM calculations. Finally, the keylock switch is used to return the PRNM to normal operation.

5.2.3.4 Q-DCIS

The NMS CIM provides dedicated redundant fiber optic serial data outputs to the Q-DCIS for the purpose of transmitting NMS data to the safety-related VDUs in the MCR and to other safety-related systems. The communication is one-way, from the NMS CIM to the Q-DCIS.

5.2.3.5 Communications with RTIF

The NMS TLU maintains a bidirectional fiber optic communication link with the RTIF TLU in the same division. The protocol has the same dynamic signal characteristics as that used for the inter-divisional trip signals. The NMS TLU transmits SRNM and PRNM trip status to the RTIF TLU over this link, and receives the reactor mode output from the RTIF TLU over this link.

6.0 STRATEGY TO MITIGATE COMMON CAUSE FAILURE

6.1 NUMAC DESIGN STRATEGY

6.1.1 Design Process

Specific actions are taken as part of the design process to minimize the likelihood of a residual design weakness that might leave the system vulnerable to common cause failure of the safety-related function.

The specific focus is driven by the hypothesis that some unanticipated set of conditions, at some time in the future, challenges the design in such a way that one or more safety-related functions in a channel is defeated. The further assumption is that since this results from "external factors" (time is an external factor), it might affect all redundant channels at the same time or in close succession, thus defeating the total system safety-related function. The total "complexity" of the overall system makes it virtually impossible to prove this cannot happen. But actions can be taken to reduce the probability to an acceptable level, and mitigate the consequences.

The issue can be divided into three general elements:

- Unexpected response to external "inputs."
- Unexpected "result" of internal processing (inside the computer controlled equipment).
- Failure to implement correctly the intended design.

The third item is addressed by the normal process, which conventionally focuses on correct implementation of the intended and identified functions. The first two, however, generally need "content" action. The NUMAC V&V process addresses the third item directly with a structured and thorough implementation process. It addresses the first two indirectly via instructions to consider abnormal conditions in defining the requirements and the design. The following paragraphs discuss the specific design aspects and methods used in the NUMAC design process.

6.1.2 General Strategy

The general strategy is:

a. Fully define performance, including abnormal conditions, both for "external" and "internal" conditions.

b. Partition the design to establish internal "boundaries" where the effects of an unanticipated operation can be detected and handled, thus reducing the complexity of the

fault detection (this allows mitigation of the effects of problems that themselves cannot be defined).

c. Establish a clear, structured process to make sure the design is correctly implemented.

The NUMAC design process directly addresses Item c., so the rest of this discussion will focus on Items a. and b.

A very basic assumption in the approach is that there are things we "don't know we don't know", and, therefore, we cannot define a direct response to them, or necessarily prevent them. However, we can define ways to mitigate the consequences of the "things", i.e., recover. (This is essentially the same philosophy practiced in the overall plant Emergency Response Procedures. The procedures address how to recover from virtually all abnormal states without ever claiming to know all the ways the plant might get into that state, or if indeed it ever will. In virtually all cases, they address conditions that the plant is not supposed to get into.) For the NUMAC Reactor Trip System, the strategy is the same -- provide a symptom based response, i.e., contain the consequences -- without ever claiming to know exactly how the system will get into that state.

6.1.3 Unexpected Response to External Inputs

This issue frequently gets lumped into "software" problems, but is really a requirements definition issue. Requirements tend to define required response to normal inputs, but frequently leave undefined expected response to at least some "abnormal" input scenarios. The action taken to address this issue is to include in the design definition process explicit definitions for every input to the equipment, both the normal range of input values (including both static and dynamic characteristics) and the abnormal range, and define the actions required for abnormal values. A review of the requirements includes a specific step to look at these definitions. These actions are taken to eliminate input conditions for which there is no defined output.

6.1.4 Unexpected "Result" of Internal Processing

This item requires two approaches, one related to specifications and one related to design structure. The first part is really the same as the above, except it applies to "inputs" to internal software modules. Every parameter passed from one processing element to another should have a "closed set" definition, i.e., normal range and abnormal range, with a defined response for all values. No value should be assumed to be "not possible" unless it literally is not possible. The actions taken to address this issue are the same as discussed above.

The rest of this discussion will focus on specific design strategies to contain and manage the consequences of problems that may slip through in spite of the above actions.

6.1.5 Design Approaches to Mitigate Consequences

The following list is NOT a list of all good design practices for embedded software machines. It is, however, a list of approaches that can significantly reduce the risk of an unacceptable

consequence of a common cause design problem and allow the individual channels to recover independently. The order of listing is not intended to provide any particular priority or order of significance.

1) Divide the software functions in the NUMAC into tasks.

This is not special per se, but a few particular aspects are. The important part about tasks is that the time required to execute them can be defined, generally maximum and minimum. If a task takes a longer or shorter time to execute than expected, then that is an indicator of a lack of complete understanding of the design. Therefore, all NUMAC designs must have the specific times defined, have those times specifically evaluated during the design process, and then have them continuously monitored by self-test. This is intended to detect abnormal operation paths in the software.

The objective is to define tasks that will run with a predefined execution time so that deviations can be detected and that tasks, once started, will run to completion, so that a lack of task completion can be detected.

The first part, in general, requires only the time monitoring. The second part, however, requires some thought on how the task steps are actually structured. For example, the "flag" or "marker" used to show that the task has run (typically monitored by the watchdog task) should be set as virtually the last step in the task to avoid somehow going into a sub-loop that leaves out some step.

The above applies to tasks that run normally. Some tasks run only on demand, such as at startup. For these, since it is virtually impossible to defend a claim that a task will not, under any circumstances, run when not intended, then the tasks need to be defined so that if a task does run unexpectedly, the consequences are acceptable (doesn't change either any values or response time outside acceptable limits) or the unplanned execution will be detected and automatically compensated for (restart or trip).

2) Watchdog timer.

The NUMAC software task structure discussed above directly supports the watchdog timer. The watchdog timer is intended to detect any task not executing at the normal rate, and then to force action that will result either in recovery or a trip (or both). To make this happen, the watchdog timer is "linked" to each task, even the non-critical ones (including self-test). The link to non-critical tasks is important because failure to execute any task indicates something is abnormal, and the objective is to detect unexpected behavior and execute mitigating action. This is a diverse monitor in that it is hardware monitoring the software.

3) Dynamic coupling to the outputs.

Dynamic coupling to the outputs is intended as a more direct (than watchdog timer) monitor of execution of critical functions, and provides a simple, diverse hardware monitor of the critical software functions. It includes a hardware time-out on the I/O

module which is required to be updated with different (hence dynamic) information at a regular rate, without which the monitor automatically, independent of software, goes to a safe trip condition.

To make this approach effective requires careful structuring of the tasks and, in particular, the steps accomplished by the high level task. The objective is to have update of the I/O module confirm that (1) the main task did run, and (2) since the main task ran, the necessary decisions were made. This is a "bootstrapping" process to gain confidence by observing, with simple monitors, that more complicated processes are still functioning.

6.1.6 NUMAC Design Strategy Summary

Full defense-in-depth NUMAC design strategy involves a combination of (1) plan for abnormal conditions that can be defined, (2) design to mitigate the consequences of abnormal conditions that could not be anticipated, and (3) use a disciplined design process to maximize the degree to which requirements are faithfully implemented in the design of the NUMAC system.

6.2 DEFENSE-IN-DEPTH AND DIVERSITY

The ESBWR includes defense-in-depth and diversity design considerations (Reference 8-14), and also has included a Diverse Protection System using both manual action and nonsafety diverse systems to provide means to accomplish the function that could otherwise be defeated by the common cause failure such as common mode software failure. The above design measures including the inclusion of the Diverse Protection System meet the requirements of RG 1.152 on common cause failure and the guidance of BTP HICB – 19.

7.0 QUALITY ASSURANCE PROGRAMS

7.1 GENERAL

The USNRC-accepted GE Quality Assurance Program (Reference 8-5) with its implementing procedures constitute the Quality Assurance system that is applied to all NUMAC products. It satisfies all applicable requirements of the following:

- 10 CFR 50 Appendix B
- ANSI/ASME NQA-1
- ISO 9001

7.2 HARDWARE

In general, hardware design and procurement control is performed in accordance with GE's normal design control program documented in GE's Engineering Operating Procedures. These procedures cover design control and documentation, verification, testing, design reviews, design records, and design change control.

7.3 SOFTWARE

Software development, verification and validation, and software configuration management shall be conducted in accordance with the software quality assurance program established for the ESBWR in the DCD (Reference 8-6), Appendix 7B. The ESBWR Software Management Plan (Reference 8-16) and the ESBWR Software Quality Assurance Plan (Reference 8-17) define software quality assurance program for the ESBWR.

8.0 REFERENCES

8-1 NEDC-32410P-A, "Nuclear Measurement Analysis and Control Wide Range Neutron Monitoring System (NUMAC-PRNM), Retrofit Plus Option III Stability Trip Function" Licensing Topic Report, GE Nuclear Energy, Class III (proprietary), October 1995.

8-2 NEDO-31439-A, "The Nuclear Measurement Analysis and Control Wide Range Neutron Monitoring System (NUMAC-WRNMS)," Licensing Topic Report, GE Nuclear Energy, Class I (non-proprietary), October 1990.

8-3 NEDE-24362-1-P, Revision 1, "General Electric Environmental Qualification Program," General Electric Company, Class III (proprietary), January 1983.

8-4 EPRI TR-102323 (TR-1003697), "Guidelines for Electromagnetic Interference Testing of Power Plant Equipment", Revision 3, November 2004

8-5 NEDO-11209-04A, "Nuclear Energy Business Group Boiling Water Reactor (BWR) Quality Assurance Program Description (Revision 4)", General Electric Company, December 31, 1982.

8-6 26A6642, ESBWR Design Control Document, Tier 2

8-7 USNRC Regulatory Guide 1.97, Revision 4, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants

8-8 NEDO-33294, "ESBWR Safety Criteria for Instrumentation and Control Systems", Revision 0

8-9 26A6641, ESBWR Design Control Document, Tier 1

8-10 MIL-STD-461D, Requirements for the Control of Electromagnetic Interference Emissions and Susceptibility

8-11 MIL-STD-462D, Test Method Standard for Measurement of Electromagnetic Interference Characteristics

8-12 IEC Standard 61000-4-X Series, Electromagnetic Compatibility for Industrial-Process Measurement and Control Equipment.

8-13 EPRI NP-5652, Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Application (NCIG-07)

8-14 NEDO-33251, "ESBWR I&C Defense-in-Depth and Diversity Report", Revision 0, July 2006

8-15 GE Nuclear Energy, "General Electric Instrument Setpoint Methodology", NEDC-31336P-A, Class III (proprietary), September 1996

8-16 NEDO-33226, "ESBWR Software Management Plan"

8-17 NEDO-33245, "ESBWR Software Quality Assurance Plan"

APPENDIX A – COMPARISON TO NUMAC APPLICATIONS PREVIOUSLY REVIEWED BY THE USNRC

Variable	*Log Rad Monitor (LRM)/ Generic*	*Wide Range Neutron Monitor (WRNM)/ Generic*	*Reactor Building Vent Radiation Monitor (RBVRM)/ Browns Ferry*	*Lead Detection Monitor (LDM)/ Brunswick*	*Power Range Neutron Monitor (PRNM)*	*Application of NUMAC For ESBWR Reactor Trip System*
Type of submittal/ review	Topical Report (NEDO 30883-A)	Topical Report (NEDO-31439-A)	Plant Specific	Plant Specific	Topical Report (NEDC-32410P-A)	Topical Report
NRC Review completed	1985	1990	1993	1993	1995	Not Applicable
Primary plant function	Monitor gamma radiation from main steam line or containment; generate trip signals when level exceeds limits.	Monitor neutron flux for startup (source and intermediate) range using fixed incore detectors; generate trip signals when level or rate of increase exceeds limits.	Monitor gamma radiation in the reactor building; generate trip signals when level exceeds limits.	Monitor temperatures measured by thermocouples in various zones in the plant; monitor RWCU flows and temperatures; generate trip signals when temperatures or differential flows exceed limits.	Monitor neutron flux for BWR power range using incore detectors; generate trip signals when level exceeds limits.	NMS – Same as WRNM and PRNM RTIF – Monitor various plant process signals and initiate an automatic reactor scram and / or main steam isolation whenever a monitored process variable exceeds limits.
Primary plant safety function	Input to reactor protection system	Input to reactor protection system; post accident confirmation of shutdown (Reg. Guide 1.97 Flux indication)	Close reactor building vents on high radiation.	Close valves or similar devices to isolate zones indicating high temperatures (indication of steam leakage in the zone).	Input to reactor protection system	NMS - Provide SRNM and PRNM trip inputs to RTIF RTIF - Provide RPS automatic scram function and MSIV isolation
Number of system channels	Four	Six or eight	Two	Two	Four/six/eight	Four

Application of Nuclear Measurement Analysis and Control (NUMAC) for the ESBWR Reactor Trip System

Variable	*Log Rad Monitor (LRM)/ Generic*	*Wide Range Neutron Monitor (WRNM)/ Generic*	*Reactor Building Vent Radiation Monitor (RBVRM)/ Browns Ferry*	*Lead Detection Monitor (LDM)/ Brunswick*	*Power Range Neutron Monitor (PRNM)*	*Application of NUMAC For ESBWR Reactor Trip System*
Primary instrument functions	Process input from one ion chamber gamma detector. Compare signal to limits and present displays and trip outputs based on results.	Process input from one neutron incore detector. Compare signal and rate of change of signal to limits and present displays and trip outputs based on results.	Process input from four remote detector signal processing units (sensor and converter). . Compare signals to limits and present displays and trip outputs based on results.	Process inputs from up to 36 thermocouples. Process inputs from 3 thermocouples and calculate differential flows. Compare signals to limits and present displays and trip outputs based on results.	Process inputs from up to 24 LPRM incore neutron detectors. Receive status inputs from other devices and processed signals from other PRNM chassis. Compare trips and present displays and trip outputs based on various algorithms.	NMS – Same as WRNM and PRNM RTIF – Similar to PRNM. Process inputs from various sensors. Receive status inputs from other devices and processed signals from other RTIF chassis. Compare trips and present displays and trip outputs based on various algorithms.

Variable	*Log Rad Monitor (LRM)/ Generic*	*Wide Range Neutron Monitor (WRNM)/ Generic*	*Reactor Building Vent Radiation Monitor (RBVRM)/ Browns Ferry*	*Lead Detection Monitor (LDM)/ Brunswick*	*Power Range Neutron Monitor (PRNM)*	*Application of NUMAC For ESBWR Reactor Trip System*
Hardware Chassis	Standard NUMAC chassis (15 card slots with 2 LVPS)	Same as LRM	Same as LRM	Same as LRM	NUMAC "wide body" chassis (21 card slots, no LVPS). Chassis is the same as the original NUMAC chassis except that LVPS are moved to remote assembly and motherboard is extended to include 5 more card slots. Mechanical design is improved with better EMI resistance.	Similar to PRNM NUMAC "wide body" chassis with external power supplies.
Key-board/ display[1]	Standard small display	Standard small or large display	Standard large display	Standard large display	Standard large display	Not Applicable User interface via Local Display Unit
Main CPU[2]	Standard NUMAC 80C86 CPU Module.	Same as LRM.	Same as LRM.	Same as LRM.	Standard NUMAC 80C386SX CPU Module. Same bus interface and general architecture as 80C86 CPU Module.	Pentium class CPU with improved bus interface

Variable	*Log Rad Monitor (LRM)/ Generic*	*Wide Range Neutron Monitor (WRNM)/ Generic*	*Reactor Building Vent Radiation Monitor (RBVRM)/ Browns Ferry*	*Lead Detection Monitor (LDM)/ Brunswick*	*Power Range Neutron Monitor (PRNM)*	*Application of NUMAC For ESBWR Reactor Trip System*
Display CPU[3]	Standard NUMAC NSC800 CPU Module	Standard NUMAC NSC800 CPU Module or standard NUMAC 64180 CPU module.	Standard NUMAC 64180 CPU Module.	Standard NUMAC 64180 CPU Module.	Standard NUMAC 64180 CPU Module.	Not Applicable
Pre-processors	N/A	N/A	87C51[4] (part of sensor and converter unit – runs at 11 MHz).	N/A	Standard NUMAC ASP Module[5] (runs at 20 MHz).	Same as PRNM, except for minor modification to accommodate new bus interface
General digital and analog I/O[6]	Standard NUMAC Modules	Standard NUMAC Modules	Standard NUMAC Modules	Standard NUMAC Modules	Standard NUMAC Modules	Same as PRNM, except for minor modification to accommodate new bus interface
Safety critical I/O	Later version has fail safe[7] monitor of CPU interface	Fail safe[7] monitor of CPU interface	Fail safe[7] monitor of CPU interface	Fail safe[7] monitor of CPU interface	Fail safe[7] monitor of CPU interface	Same as PRNM
Communications with other NUMAC instruments	N/A	N/A	N/A	N/A	NUMAC fiber optic "reflected memory" interface module	NUMAC dual counter-rotating fiber optic "replicated memory network"

Variable	*Log Rad Monitor (LRM)/ Generic*	*Wide Range Neutron Monitor (WRNM)/ Generic*	*Reactor Building Vent Radiation Monitor (RBVRM)/ Browns Ferry*	*Lead Detection Monitor (LDM)/ Brunswick*	*Power Range Neutron Monitor (PRNM)*	*Application of NUMAC For ESBWR Reactor Trip System*
Communications between channels for two-out-of-four voting of trips	N/A	N/A	N/A	N/A	MIL-Std-1553 point-to-point fiber optic data links.	MIL-Std-1553 point-to-point fiber optic data links. Similar to PRNM
Main CPU monitor	"Watch-dog" timer	Same as LRM	Same as LRM	Same as LRM	Same as LRM	Same as PRNM
Separation in chassis	Serial data link plus analysis	None. All hardware qualified.	None. All hardware qualified.	None. All hardware qualified.	None. All hardware qualified.	Same as PRNM
System separation	Accomplished external to the chassis, unchanged from pre-NUMAC.	Fiber optic for new interfaces. Remaining accomplished external to the chassis, unchanged from pre-NUMAC.	Accomplished external to the chassis, unchanged from pre-NUMAC.	Accomplished external to the chassis, unchanged from pre-NUMAC.	All inter-channel and new interfaces use fiber optic. Remaining accomplished external to the chassis, unchanged from pre-NUMAC.	Similar to PRNM. All interfaces between channels and interfaces with external systems use fiber optics.
Peripheral devices	None	Signal preamplifier; remote digital operator display (optional)	Sensor and Converters; Auxiliary alarm units; final relay interface panels	Iso-thermal interface panels; final output relay interface panels	Rod block monitor/plant computer interface chassis; final output relay interface panels; 2/4 voter	SRNM Detector Preamplifier (same as WRNM) BPU, OLU, Load Drivers

Variable	*Log Rad Monitor (LRM)/ Generic*	*Wide Range Neutron Monitor (WRNM)/ Generic*	*Reactor Building Vent Radiation Monitor (RBVRM)/ Browns Ferry*	*Lead Detection Monitor (LDM)/ Brunswick*	*Power Range Neutron Monitor (PRNM)*	*Application of NUMAC For ESBWR Reactor Trip System*
Software V&V Program	NUMAC V&V Program Ver. 1	NUMAC V&V Program Ver. 3	NUMAC V&V Program Ver. 3	NUMAC V&V Program Ver. 3	NUMAC V&V Program Ver. 3	ESBWR V&V Program
Main CPU -- Operating System	NUMAC NM86.	Same as LRM	Same as LRM	Same as LRM	NUMAC NM386. Minor adaptation of NM86 to run on 80C386SX CPU.	Minor adaptation of NM386 to run on Pentium class CPU
-- Application S/W	PL/M 86 and ASM	Same as LRM	Same as LRM	Same as LRM	Same as LRM plus "C"	Same as PRNM
-- Application structure	Tasks with priorities -- prime functions in highest priority.	Same as LRM	Same as LRM	Same as LRM	Same as LRM	Same as PRNM
Display CPU -- Operating System	N/A – executive loop.	Same as LRM	Same as LRM	Same as LRM	Same as LRM	Not Applicable
-- Application S/W	Pascal and ASM	Same as LRM	Same as LRM	Same as LRM	Same as LRM	Not Applicable
Pre-processor CPU -- Operating system	N/A	N/A	N/A – executive loop	N/A	N/A – executive loop	Same as PRNM
-- Application S/W	N/A	N/A	ASM	N/A	ASM	Same as PRNM

Table Notes:

1. "Small" display is 128 by 512 pixels. "Large" display is 256 by 512 pixels.

2. The NUMAC 80C86 CPU module runs at 3 MHz. The NUMAC 80C386SX CPU module runs at 16 MHz. The interface with the NUMAC motherboard bus is the same for both.

3. The NUMAC NSC800 CPU module runs at 5 MHz, and is used with the small display. The NUMAC 64180 CPU module runs at 12 MHz and is used with the large display. Both communicate with the Main CPU over a serial data bus, and have no direct communication with other modules, and do not communicate with the motherboard parallel bus.

4. The sensor and converter pre-processor (RBVRM) communicates over a serial RS422 data link with an RS422 module in the chassis, which, in turn, communicates with the main CPU via shared memeory over the parallel data bus in the motherboard.

5. The NUMAC ASP Module (contains DSP56001 CPU) communicates with the main CPU via shared memory over the parallel data bus in the motherboard.

6. All general I/O modules communicate with the main CPU via the parallel data bus in the motherboard. The specific combination of modules varies with the specific application.

7. The "fail safe monitor" for the computer interface is a dynamic monitor located on the output module that requires the computer to continuously update the output control, with a changing signal. If the computer fails to update the output within a limited time, the output automatically goes to a pre-defined "trip" state.

APPENDIX B – SYSTEM BLOCK DIAGRAMS

(To be included in next revision)

APPENDIX C – FAILURE MODES AND EFFECTS ANALYSIS

(To be included in next revision)