LICENSE AMENDMENT REQUEST TO IMPLEMENT PRNM/ARTS/MELLLA – REVISED REPORTS
Attachment 2

NEDO-33685
Revision 2

December 2012

DIGITAL I&C-ISG-06 COMPLIANCE FOR COLUMBIA GENERATING STATION NUMAC POWER RANGE NEUTRON MONITORING RETROFIT PLUS OPTION III STABILITY TRIP FUNCTION

HITACHI

GE Hitachi Nuclear Energy

NEDO-33685
Revision 2
DRF Section 0000-0141-6924-R2
December 2012

Non-Proprietary Information-Class I (Public)

Digital I&C-ISG-06 Compliance for Columbia Generating Station NUMAC Power Range Neutron Monitoring Retrofit Plus Option III Stability Trip Function

PROPRIETARY INFORMATION NOTICE

This is a non-proprietary version of the document NEDC-33685P, Revision 2, which has the proprietary information removed. Portions of the document that have been removed are indicated by an open and closed bracket as shown here [[ ]].

IMPORTANT NOTICE REGARDING CONTENTS OF THIS REPORT

Please Read Carefully

The design, engineering, and other information contained in this document is furnished for the purpose of supporting the Columbia Generating Station license amendment request for a power range neutron monitor system upgrade in proceedings before the U.S. Nuclear Regulatory Commission. The only undertakings of GEH with respect to information in this document are contained in the contracts between GEH and its customers or participating utilities, and nothing contained in this document shall be construed as changing that contract. The use of this information by anyone for any purpose other than that for which it is intended is not authorized; and with respect to any unauthorized use, GEH makes no representation or warranty, and assumes no liability as to the completeness, accuracy, or usefulness of the information contained in this document.

Revision Summary

Revision	Change Summary
0	Initial Revision
1	Updated revision numbers in the references section for NEDC-33694P, NEDC-33697P, and NEDC-33698P.
2	Correction to APRM bypass in Section 9.2.8.3.

Table of Contents

Table of Tables

Table of Figures

Acronyms and Abbreviations

Term	Definition
ABB	ASEA Brown Boveri
ADAMS	Agency-wide Documents Access and Management System
A/D	Analog to Digital
AFV	As-Found Value
AL	Analytic Limit
ALV	As-Left Value
ANSI	American National Standards Institute
AOO	Anticipated Operational Occurrence
APRM	Average Power Range Monitor
ARTS	Average Power Range Monitor, Rod Block Monitor Technical Specification Improvement Program
ASP	Automatic Signal Processor
ATWS	Anticipated Transient Without Scram
AV	Allowable Value
BTP	Branch Technical Position
BWR	Boiling Water Reactor
BWROG	Boiling Water Reactors Owners Group
CAL	Calibrate
CCF	Common-Cause Failure
CEO	Chief Executive Officer
CFR	Code of Federal Regulations
CGS	Columbia Generating Station
CI	Configurable Item
CMR	Calculation Modification Record
COLR	Core Operating Limits Report
CP	Common Procedure
CTP	Core Thermal Power
D/A	Digital to Analog
D3	Diversity and Defense-in-Depth

Term	Definition
DBE	Design Basis Event
DDR	Detailed Design Review
ΔP	Differential Pressure
DI&C-ISG	Digital Instrumentation & Control-Interim Staff Guidance
DRF	Design Record File
DSP	Digital Signal Processor
DVR	Design Validation Review
EAROM	Electrically Alterable Read Only Memory
EEPROM	Electrically Erasable Programmable Read-Only Memory
EL	Electro-luminescent
ELD	Electro-Luminescent Graphics Display
EMC	Electromagnetic Compatibility
EMI	Electromagnet Interference
ENW	Energy Northwest
EOP	Engineering Operating Procedure
EPRI	Electric Power Research Institute
EPROM	Electronic-Programmable Read-Only Memory
ERM/ECN	Engineering Review Memorandum/Engineering Change Notice
ESD	Electrostatic Discharge
EWP	Engineering Work Plan
FAT	Factory Acceptance Testing
FDDI	Fiber Direct Data Interface
FO	Fiber Optic
FRD	Firmware Release Description
FT	Flow Transmitter
GAF	Gain Adjustment Factor
GDC	General Design Criteria
GEDAC	General Electric Data Acquisition & Communication
GEH	GE-Hitachi Nuclear Energy Americas LLC.
GGNS	Grand Gulf Nuclear Station

Term	Definition
HFE	Human Factors Engineering
HVAC	Heating, Ventilating, and Air Conditioning
HVPS	High Voltage Power Supply
I&C	Instrumentation and Control
IEEE	Institute of Electrical and Electronics Engineers
I/O	Input/Output
INOP	Inoperative
ISA	Instrument Society of America
ISG	Interim Staff Guidance
I/V	Current/Voltage
IV&V	Independent Verification and Validation
LAR	License Amendment Request
LAT	Leave Alone Tolerance
LCS	Licensee Controlled Specifications
LER	Licensee Event Report
LIM	LPRM Input Modules
LOCA	Loss-of-Coolant Accident
LPRM	Local Power Range Monitor
LSSS	Limiting Safety System Setting
LTR	Licensing Topical Report
LTSP	Limiting Trip Setpoint
LVPS	Low Voltage Power Supply
MCR	Main Control Room
MELLLA	Maximum Extended Load Line Limit Analysis
NIC	NUMAC Interface Computer
NMS	Neutron Monitoring System
NQA	Nuclear Quality Assurance
NRC	Nuclear Regulatory Commission
NRT	NUMAC Review Team
NTSP	Nominal Trip Setpoint

Term	Definition
NUMAC	Nuclear Measurement Analysis and Control
NUREG	Nuclear Regulatory Commission Regulation
NVRAM	Non-Volatile Random Access Memory
ODA	Operator Display Assembly
OEM	Original Equipment Manufacturer
OL	Operating Limit
OPRM	Oscillation Power Range Monitor
P&L	Profit &Loss
P&P	Policies and Procedures
PDMS	Product Data Management System
PL	Programmable Logic
PLC	Programmable Logic Controller
PLD	Programmable Logic Device
PEA	Primary Element Accuracy
PM	Project Manager
PMA	Process Measurement Accuracy
PO	Purchase Order
PPC	Plant Process Computer
PQC	Product Quality Certification
PRM	Power Range Monitor
PRNM	Power Range Neutron Monitor
PRNMS	Power Range Neutron Monitoring System
PRR	Product Requirements Review
PWP	Project Work Plan
QA	Quality Assurance
QLVPS	Quad LVPS
RAM	Random Access Memory
RBM	Rod Block Monitor
RCCE	Responsible Configuration Control Engineer
RE	Responsible Engineer

Term	Definition
RFI	Radio Frequency Interference
RG	Regulatory Guide
RM	Responsible Manager
ROM	Read Only Memory
RPS	Reactor Protection System
RRS	Required Response Spectra
RTP	Rated Thermal Power
RV	Responsible Verifier
SCC	Successive Confirmation Count
SCMP	Software Configuration Management Plan
SDOE	Secure Development and Operational Environment
SDP	Software Development Plan
SE	Safety Evaluation
SMP	Software Management Plan
SOP	Software Operations Plan
SQAP	Software Quality Assurance Plan
SR	Surveillance Requirement
SRP	Standard Review Plan
SRSS	Square Root of the Sum of the Squares
STA	Spurious Trip Avoidance
STP	Simulated Thermal Power
STS	Standard Technical Specifications
SVVP	Software V&V Plan
SW	Service Water
TCP/IP	Transmission Control Protocol/Internet Protocol
TI	Test Instruction
TID	Total Integrated Dose
TRS	Test Response Spectra
TS	Technical Specifications
UFSAR	Updated Final Safety Analysis Report

Term	Definition
V&V	Verification and Validation
VAC	Alternating Current Electrical Voltage
VDC	Direct Current Electrical Voltage

Executive Summary

The following document provides Digital Instrumentation and Control-Interim Staff Guidance (DI&C-ISG)-06 Compliance for the Columbia Generating Station PRNMS. This compliance document includes Phase 1 and a majority of Phase 2 documentation required to support the CGS PRNM license amendment request.

1. Summary Description

Energy Northwest (ENW) is replacing the existing analog Power Range Monitor (PRM) subsystem of the existing Neutron Monitoring System (NMS) with the more reliable, digital Nuclear Measurement Analysis and Control (NUMAC) Power Range Neutron Monitoring System (PRNMS) at Columbia Generating Station (CGS) during the Spring 2013 refueling outage. The NUMAC PRNMS retrofit is based on the Reference 1 Licensing Topical Report (LTR), which was approved by Nuclear Regulatory Commission (NRC) (Reference 2). The PRNM System design retrofit includes an automatic instability trip function, Oscillation Power Range Monitor (OPRM), which is defined by the Boiling Water Reactor Owners' Group (BWROG) as OPRM Option III detect-and-suppress function. Thus, CGS will be transitioning from the ASEA Brown Boveri (ABB) Option III stability solution to the GEH Option III stability solution.

As noted in Reference 1, the Local Power Range Monitor (LPRM) detector signal processing, LPRM averaging, Average Power Range Monitor (APRM) trips, Rod Block Monitor (RBM) logic and interlocks are retained. However, the six APRM channel configuration is replaced with four APRM channels, each channel utilizing 1/4 total LPRM detectors. APRM functions are retained, but four 2-Out-Of-4-voter channels are added, two supplying inputs to each Reactor Protection System (RPS) trip system. The trip outputs from the four APRM channels are sent to each of the four voter channels, thus each input to RPS is a voted result of all four APRMs.

The Option III stability solution combines closely spaced LPRM detectors into "cells" to effectively detect either core-wide or regional modes of reactor instability. These cells are termed OPRM cells and are configured to provide local area coverage with multiple channels. The OPRM cell signals are analyzed by the Option III detection algorithm to determine when a reactor trip is required.

1.1 System Description

The CGS PRM is to be replaced with the NUMAC PRNM system. All current PRM functions are retained, including LPRM detector signal processing, LPRM averaging, APRM trips, and RBM logic and interlocks. The current analog LPRM signal processing electronics, LPRM averaging and APRM trip electronics, LPRM detector power supply hardware and recirculation flow signal processing electronics are being replaced by integrated digital NUMAC chassis based APRM electronics. The six APRM channels are replaced with four channels of NUMAC APRM. Four 2-Out-Of-4 voter channels are added between the APRM channels and the existing RPS logic, but do not change the actual RPS interface or trip logic. Note all interfaces with external systems are maintained electrically equivalent using interface sub-assemblies with exception of the interface to the plant computer and plant operator's panel. Interface to the plant computer system is accomplished by the NUMAC Interface Computer (NIC) system and Operator Display Assemblies (ODAs) replace meters and indicators. The NUMAC PRNM subsystems consist of an APRM, RBM, OPRM, and Bypass Switch. Detailed descriptions of these subsystems and additional processing changes are described below.

1.2 Detailed System Description

APRM

The APRM System is divided into four APRM channels and four 2-Out-Of-4 voter channels. Each APRM channel provides inputs to each of the four voter channels. The four voter channels are divided into two groups of two, with each group of two providing inputs to one RPS trip system. The system is designed to allow one APRM channel, but no voter channels, to be bypassed. A trip from any one unbypassed APRM will result in a "half-trip" in all four of the voter channels, but no trip inputs to either RPS trip system. Because APRM trip functions Neutron Flux-High (Setdown), Simulated Thermal Power (STP)-High, Neutron Flux-High and OPRM Upscale are implemented in the same hardware, these trip functions are combined with APRM INOP trip function. Any function trip, such as Neutron Flux-High (Setdown), STP-High, Neutron Flux-High or INOP trips, from any two unbypassed APRM channels will result in a full trip in each of the four voter channels, which in turn results in two trip inputs into each RPS trip system logic channel (A1, A2, B1, and B2). Similarly, any INOP or OPRM Upscale trip from any two unbypassed APRM channels will result in a full trip from each of the four voter channels. Three of the four APRM channels and all four of the voter channels are required to be OPERABLE to ensure that no single failure will preclude a scram on a valid signal. In addition, to provide adequate coverage of the entire core, consistent with the design bases for the APRM functions Neutron Flux-High (Setdown), STP-High, and Neutron Flux-High, at least 20 LPRM inputs, with at least three LPRM inputs from each of the four axial levels at which the LPRMs are located, must be operable for each APRM channel.

Flow Processing

The existing PRM flow electronics receives eight flow signal inputs, each one representing the flow of loop A or loop B. Four separate flow units, two per RPS trip system, receive two transmitter inputs each, one from loop A and the other from loop B. For the replacement PRNM system, each transmitter output signal is routed to one of the four APRM chassis, and each APRM processes and sums two transmitter signals, one from loop A and the other from loop B, for a total flow signal. [[

]]

Rod Block Monitor & Control Rod Block

Deletion of the APRM rod blocks from the Technical Specifications (TS) was independent of this PRNM replacement. The APRM rod blocks reside in the CGS Licensee Controlled Specifications (LCS) in accordance with Nuclear Regulatory Commission Regulation (NUREG)-1433 (Reference 3).

[[

]]

OPRM

The OPRM Upscale Function receives input signals from the LPRMs within the reactor core, which are combined into "cells" for evaluation by the OPRM algorithms.

The OPRM Upscale Function is enabled when thermal power is greater than or equal to the value specified in the Core Operating Limits Report (COLR) and core flow is less than the value specified in the COLR. Within this operating region actual thermal-hydraulic oscillations may occur. The OPRM Upscale Function is required to be operable when the power is greater than or equal to the OPRM operable value specified in the COLR. This is the region of power-flow operation where anticipated events could lead to thermal-hydraulic instability and related neutron flux oscillations. An OPRM Upscale trip is issued from an APRM channel when the period based detection algorithm in that channel detects oscillatory changes in the neutron flux, indicated by the combined signals of the LPRM detectors in a cell, with period confirmations and relative cell amplitude exceeding specified setpoints. One or more cells in a channel exceeding the trip conditions will result in a channel trip. An OPRM Upscale trip is also issued from the channel if either the growth rate or amplitude based algorithms detect growing oscillatory changes in the neutron flux for one or more cells in that channel.

BYPASS

As described in Section 4.4.1.1.1 of Reference 1, [[

]] Administrative controls for the bypass switch are discussed below in Section 1.4.6.

1.3 Regulatory Evaluation

Digital system real-time system architectures in instrumentation and control (I&C) systems are contained in Branch Technical Position (BTP) 7-21, "Guidance on Digital Computer Real-Time Performance." Additional architectural descriptions is contained in the Standard Review Plan (SRP) BTP 7-14 Section B.3.3.2, "Design Activities - Software Architecture Description." Section B.3.3.2 states that the Architecture Description should support the understanding of the functional and performance characteristics credited, and that NUREG/CR-6101 (ADAMS Accession No. ML072750055), Section 3.3.1 "Hardware and Software Architecture," and Section 4.3.1, "Hardware/Software Architecture Specifications," contain relevant guidance.

1.4 Hardware and Module Descriptions

NEDC-33696 (Reference 4) contains information on the CGS PRNM hardware architecture description.

1.4.1 Processor Subsystem

1.4.1.1 386SX Functional Processor

As described in Section 5.3.3.1 of Reference 1, [[

]]

1.4.1.2 Display Controller Module

As described in Section 5.3.3.2 of Reference 1, [[

]]

1.4.1.3 Scanning ASP Processor

As described in Section 5.3.3.6 of Reference 1, [[

]]

1.4.1.4 Stability ASP Processor

As described in Section 5.3.3.6 of Reference 1, [[

]]

1.4.2 Safety Function Processor

1.4.2.1 386SX Computer Module

As described in Section 5.3.3.1 of Reference 1 [[

]]

1.4.3 Input/Output (I/O) Modules

1.4.3.1 LPRM Input Module

As described Section 5.3.3.4 of Reference 1, [[

]]

1.4.3.2 Open Drain I/O Module

As described in Section 5.3.3.5 of Reference 1, [[

]]

1.4.3.3 16-Channel Analog Output Module

As described in Section 5.3.3.7 of Reference 1, [[

]]

1.4.3.4 Analog Module

As described in Section 5.3.3.8 of Reference 1, [[

]]

1.4.4 Communication Modules

1.4.4.1 FDDI Communication Module

As described in Section 5.3.3.9 of Reference 1, [[

]]

1.4.4.2 GE I/O Communication Module

As described in Section 5.3.3.10 of Reference 1, [[

]]

1.4.4.3 General Electric Data Acquisition & Communication (GEDAC) Module

As described in Section 5.3.3.12 of Reference 1, [[

]]

1.4.4.4 Broadcaster Module

As described in Section 5.3.3.13 of Reference 1, [[

]]

1.4.5 Voters

1.4.5.1 2-Out-Of-4 Logic Module

As described in Section 5.3.2.3 and 5.3.3.17 of Reference 1, [[

]]

1.4.5.2 Two-Out-of-Four Fiber-Optic Interface Card

As described in Section 5.3.3.18 of Reference 1, [[

]]

1.4.5.3 Relay Card Module

As described in Section 5.3.3.19 of Reference 1, [[

]]

1.4.6 Manual or Administrative Controls

The PRNM system interfaces will be solely located in the Main Control Room (MCR) at CGS. In accordance with plant procedures, access to the MCR is limited to those with approval from station management and controlled by the use of key cards. CGS's Operating Policies, Programs, and Practices Procedure dictates under what circumstances and who is allowed to operate equipment in the MCR. By procedure guidance, the PRNM equipment will be controlled with permission from MCR Supervision. All operations personnel and technicians who will interface with the PRNM system will be trained on its operating fundamentals and the procedures which delineate their interaction with the system. This training will incorporate classroom and simulator training prior to the startup from the outage in which the PRNM plant modification is installed.

The APRM/OPRM bypass switch will be located on panel H13-P603 in the "Operator-at-the-Controls zone" within the MCR. By procedure, entry into this area requires Control room supervision permission. The APRM/OPRM bypass switch will cause an indicator lamp to illuminate, as well as an indication of bypass status on displays at the APRM and its respective ODA. The APRM/OPRM bypass switch will be operated in accordance with plant procedures by a Licensed Reactor Operator.

The PRNM panel access will be controlled by several means in addition to the MCR controls. There are three modes in which the PRNM panels can be used to manipulate the equipment, INOP-CAL, INOP-SET, and OPER-SET. [[

]]

LPRM gain values and Core Thermal Power (CTP) values will be determined in accordance with plant procedures. Plant personnel will be required by procedure to obtain Operations supervision permission to upload the LPRM gain and CTP values into the PRNM as per the administrative controls described above ([[ ]]).

1.4.7 Power Supply

1.4.7.1 High Voltage Power Supply Module

As described in Section 5.3.3.3 of Reference 1, [[

]]

1.4.7.2 Low Voltage Power Supply Module

As described in Section 5.3.3.16 of Reference 1, [[

]]

1.4.7.3 Quad Power Supply

Per Section 5.3.2.6 of Reference 1 and Section 4.2.3 of Reference 5, [[

]]

1.4.8 Test Subsystem

As described in Section 5.3.11 of Reference 1, [[

]]

1.4.9 Other Subsystems

1.4.9.1 NUMAC Interface Computer

[[

]]

1.4.9.2 Operator Display Assembly

[[

]]

1.4.10 Cabinets, Racks, and Mounting Hardware

As described in Section 5.3.1 of Reference 1, [[

]]

Each APRM, RBM and Quad LVPS chassis is of a modular design to facilitate calibration, maintenance and replacement of modules. Upon slide out of the instrument, all modules are accessible for removal and replacement. All required cable installations are possible with the instrument in the withdrawn position. Each APRM, RBM and QLVPS chassis and each 2-Out-Of-4 Logic Module and RBM Interface Module is constructed in a sliding frame assembly. Mounting slides are installed in the existing panel, attaching to existing structures using adapter brackets after removal of original equipment. Each APRM and RBM front panel consists of an electro-luminescent graphics display (ELD), a set of input keys, a keylock switch, chassis handles and chassis retaining hardware.

1.4.11 Appendix B Compliance

Section 9.2.1 of Reference 1 states that NRC accepted the GE Quality Assurance (QA) Program (Reference 6) with its implementing procedures, which was applied to the NUMAC PRNM projects. This program satisfied the 10 CFR 50 Appendix B, ANSI/ASME Nuclear Quality Assurance (NQA)-1, and ISO 9001. As discussed in Section 2.4.5, the GEH design, manufacturing, inspection, assembly and support for Factory Acceptance Testing (FAT) at the GEH facilities, was provided in accordance with the GEH Nuclear Energy Quality Assurance Program as described in the NRC accepted revision of NEDO-11209-04A, Revision 08 (Reference 7) and GEH Nuclear Energy ISO-9001 Quality Management System Description, NEDO-33280, Revision 9 (Reference 8). The GEH Quality Assurance Program (Reference 9) has since been revised and approved by the NRC (Reference 10).

1.4.12 System Response Time

NEDC-33690P (Reference 11) evaluates the Response Time of the CGS PRNM system versus the safety analysis requirements and standard criteria for digital I&C. This evaluation demonstrates compliance with the criteria of BTP 7-21 (Reference 12) and Staff Positions 1.19 and 1.20 of DI&C-ISG-04 (Reference 13).

Plant specific requirements for time response issues are directly addressed in table items 8.3.4.4.4, 8.4.4.4.4 and 8.5.4.4.4 of Reference 14, which is included as license amendment request (LAR) Enclosure 2, Attachment 1.

1.4.13 Communications

As stated in Section 5.3.2.7 of Reference 1, [[

]] Additional detail for PRNM Communications is located in Section 7.

2. Hardware Development Process

2.1 Introduction

This Section describes the development process and the quality control process that governed the development process for the CGS PRNMS. The description includes both development of the individual functional units and modules and how those units and modules were integrated into the application-specific safety function design. The level of detail is consistent with information requirements in the Interim Staff Guidance (ISG) for the Licensing Process of Digital Instrumentation & Controls, Digital (DI&C) I&C-ISG-06 (Reference 15).

2.2 Overview

The regulatory requirements in Section 2.3 apply to digital I&C upgrades with respect to the hardware development process.

The Section 2.4 discussion supports the assertion that the CGS PRNM fulfills the criteria of DI&C ISG-06 (Reference 15), and the regulatory requirements specified below.

2.3 Regulatory Evaluation

The regulatory requirements applicable to digital I&C upgrades with respect to the hardware development process are:

10 CFR 50.55a(a)(1) "Structures, systems, and components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed," which addresses Quality Standards for Systems Important to Safety.

10 CFR 50.55a(h)(3), "Safety Systems" states: "Applications filed on or after May 13, 1999 ...must meet the requirements for safety systems in IEEE Standard 603-1991, and the correction sheet dated January 30, 1995." IEEE Standard 603 Clause 5.3 requires that components and modules be of a quality that is consistent with minimum maintenance requirements and low failure rates, and that safety system equipment be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program.

GDC 1, "Quality Standards and Records" states: "Structures, systems, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed..."

2.4 Hardware Development Process Evaluation

2.4.1 Hardware Development Scope

The NUMAC PRNM system is designed to operate in the CGS configuration as a four (4) divisional system that processes the existing LPRM signals. The PRNM system consists of APRM instruments, RBM instruments, RBM interface modules, 2-Out-Of-4 logic modules, Calibration/monitor panels, interconnecting cabling, and power supplies. Refer to Section 1.4,

Hardware Architecture Description, for a description of the CGS PRNM System hardware. Refer to Table 2-1 for a list of CGS PRNM components developed under the GEH process.

The PRNM system will communicate with the plant process computer (PPC) with specified protocols. The system will perform the Option III long-term stability function for core stability and the APRM RBM TS (ARTS)/Maximum Extended Load Line Limit Analysis (MELLLA) functions. The NUMAC PRNM system is a firmware-based system designed to allow functional flexibility while maintaining maximum reliability.

The NUMAC PRNM equipment is configured for installation into the existing CGS PRNM panels. Figure 2-1 shows the PRNM panel arrangement for the CGS PRNM panel configuration.

Figure 2-1 CGS PRNM Panel Layout Design

Bay 1	Bay 2	Bay 3	Bay 4	Bay 5
2/4 Logic Module (RPS Div B1) A11	**RBM I/F Module** (RBM A) A21	**2/4 Logic Module** (RPS Div B1) A31	**2/4 Logic Module** (RPS Div A2) A41	**2/4 Logic Module** (RPS Div A1) A51
APRM 4 AR11	**RBM A** AR21	**APRM 2** AR31	**APRM 3** AR41	**APRM 1** AR51
LPRM 4 AR12	**RBM B** AR22	**LPRM 2** AR32	**LPRM 3** AR42	**LPRM 1** AR52
APRM 4 / LPRM 4 **Cal/Mon Panel** A18	RBM A / B **Cal/Mon Panel** A28	APRM 2 / LPRM 2 **Cal/Mon Panel** A38	APRM 3 / LPRM 3 **Cal/Mon Panel** A48	APRM 1 / LPRM 1 **Cal/Mon Panel** A58
	RBM I/F Module (RBM B) A22			
Low Voltage Power Supply PS10	**Low Voltage Power Supply** PS20	**Low Voltage Power Supply** PS30	**Low Voltage Power Supply** PS40	**Low Voltage Power Supply** PS50

GEH provides a modification kit and installation hardware for the existing CGS cabinets that includes the rails, supports, slides, and fasteners to mount the NUMAC PRNM hardware. During the system Validation Testing and FAT, GEH simulated the CGS panel configuration and used the GEH supplied cable assemblies required for the site installation.

ENW will be responsible for removal of the existing equipment and the installation of the PRNM Equipment, wiring in the panel P-603 panels, and installation of the fiber-optic cabling between the P-603 and P-608 panels. Installation of the CGS PRNM system at CGS will be performed by ENW under the ENW Appendix B quality program.

Table 2-1 PRNM System Components Deliverables

Description	Part Number	System Quantity
APRM Chassis (2 per APRM Channel)	304A3719TCG001	8
RBM Chassis (1 per RBM Channel)	304A3720TCG001	2
LVPS (1 per panel Bay)	304A3721AAG001	5
2-Out-Of-4 Logic Module	304A3807TCG001	4
RBM Interface Module	304A3806TCG001	2
FO Bypass Switch	148C6420	1
LPRM Connector Panel	148C6759	13
APRM Calibration Monitoring Panel	148C7146G003	4
PRNM Cabinet Modification Kit	105E1505TCG002	1
PRNM cables	299X774TCG001	1 Lot
Miscellaneous Accessory System Parts	299X740TC	1 Lot
Panel FO cables for PRNM (Internal)	299X773TCG001	1 Lot
Panel External FO cables	299X773TCG002	1 Lot
Panel FO cables for PRNM (Spare)	299X773TCG003	1 Lot
NUMAC Interface Computer	147C3736TCG001	1
ODAs for APRM	304A3800TCG001	2
ODAs for RBM	304A3800TCG002	2
RBM Calibration Monitoring Panel	148C7155G001	1
4 Chan Analog Isolator Module	148C6130AAG001	4
Marker Plate for FO Bypass Switch	148C7149P001	2
Mounting Hardware for APRM ODAs in control room	491X688G007	1 set
Mounting Hardware for RBM ODAs in control room	491X688G008	1 set

2.4.2 Organization

The GEH project organization is presented in Section 4.4 (4.4.5.2.1 through 4.4.5.2.6). The GEH QA organization executes the QA Program by audit and inspection of activities affecting the safety-related functions. Additionally, they report to a management level that ensures independence from cost and schedule.

2.4.3 Project Management & Project Work Plan

The CGS PRNM Project Work Plan (PWP) is the GEH document that addresses the project management aspects of the Hardware Development Process.

The PWP is required by GEH procedure Engineering Operating Procedure (EOP) 25-5.00, Work Planning and Scheduling (Reference 16), for all customer contracted design work and projects. Four key purposes of the PWP and schedule are: 1) Define the scope and deliverables of the project, 2) Identify critical path items/activities that are required to complete the project, as well

as milestone dates for these items/activities, 3) Serve as a tool to monitor the project progress, and 4) Identify the required manpower and resources needed throughout the project.

Project risk management is also a key function of the PWP. The PWP invokes GEH P&P 10-29 (Reference 17), which identifies four major phases to the Risk Management practices: [[

]] Contingency planning is conducted as part of the Project Risk Analysis. A Project Risk analysis is kept in the project Design Record File (DRF) and updated at least once a month. Project Risk Management is described in detail in Section 10.3.

The PWP invokes the application of the GEH QA program for the CGS PRNM project. GEH policies and procedures, address management directives, documentation requirements, reviews and audits, testing, problem reporting and corrective action program, tools and techniques, supplier control, quality assurance records, training, and risk management. See Section 2.4.5 for more details about GEH policies and procedures.

The PWP also defines the interface between ENW (the licensee) and GEH (the vendor) for the development of the CGS PRNMS, including how ENW provides oversight of the project through reviews of project deliverables, audits, and the FAT.

2.4.4 Hardware Development

In conjunction with the PWP, the CGS PRNM Engineering Work Plan (EWP) provides a roadmap for the hardware development. The CGS PRNM design started with standard NUMAC hardware modules and chassis, and existing PRNM designs (i.e., PRNM installations at plants) and made only those modifications required to satisfy the CGS-specific requirements. The design starting points and design activities to support the PRNM hardware development are provided in the EWP.

2.4.5 Quality Assurance

GEH design, manufacture, inspection, assembly and support for FAT at the GEH facilities, was provided in accordance with the GEH Nuclear Energy Quality Assurance Program as described in the NRC accepted revision of Reference 7 and Reference 8. The provisions of 10CFR50 Appendix B and 10CFR21 apply to the GEH hardware development process.

All activities affecting quality are prescribed by documented instructions, procedures, or drawings. The instructions, procedures and drawings include acceptance criteria for determining that activities have been satisfactorily accomplished. A few examples of the GEH policies and procedures that implement the GEH QA program include:

[[

]]

Additional applicable GEH Engineering policies and procedures are identified in the PWP.

Upon completion of all testing, the QA organization issues a Product Quality Certification (PQC). [[

]] See Section 4.4.1.3 for more details about QA during the project.

The ENW QA Program governs their activities for all installation work at CGS, and the subsequent operation and maintenance of the CGS PRNM system at CGS.

2.4.6 Design Control & Configuration Management

The following are the primary GEH procedures that are used in conjunction with the design activities and plans to implement configuration management during the development of NUMAC hardware for CGS:

[[

]]

The procedures above are the primary procedures used in conjunction with the design activities and plans to establish the configuration management program for NUMAC products. The information presented above is not intended to be a comprehensive discussion of the GEH configuration management policies and procedures. A complete and comprehensive discussion of the GEH configuration management program is beyond the scope of this discussion.

2.4.7 Training

The CGS PRNM PWP identifies the project team, roles, and responsibilities. Personnel proficiency to perform the duties associated with the assigned roles is addressed by [[

]] All personnel are trained to assure proficiency in applicable quality and technical tasks prior to assignment of work activities affecting the quality of GEH products and services.

Per [[

]] The managers assure personnel are proficient in those tasks applicable to project specific work assignments. Managers assign required training for personnel based on training assessments.

Personnel performing work are trained on the applicable plans, specifications, and GEH policies and procedures. [[

]]

2.4.8 Commercial Grade Dedication

Dedication is the acceptance process undertaken to provide reasonable assurance that a commercial grade item to be used as a basic (i.e., safety-related) component will perform its intended safety-related function and, in this respect, is deemed equivalent to an item designed and manufactured under a 10CFR50 Appendix B quality assurance program. GEH achieves this

assurance by identifying the critical characteristics of the item, based on both the application and the qualification, and verifying acceptability by inspections, tests, or analyses performed by the purchaser or third-party dedicating entity after delivery. This is supplemented, as necessary, by one or more of the following: commercial grade surveys; product inspections or witness hold points at the manufacturer's facility, and analysis of historical records for acceptable performance.

[[

]]

The GEH dedication process is conducted in accordance with the applicable provisions of 10CFR50 Appendix B.

[[

]]

2.4.9 Control of Purchased Material, Equipment, and Services Procedures

GEH identifies and controls materials, parts, and components, including partially fabricated assemblies by part number or other appropriate means. This ID may be either on the item or on records traceable to the item. The ID is maintained throughout fabrication, installation, and use of the item.

The following are the primary GEH procedures that are used in conjunction for the control of purchased material, equipment, and services:

[[

]]

2.4.10 System Integration

GEH system integration activities include:

1) Developing the plant-specific design in a way that [[

]] (See Reference 1, Section 5.3.5.5 and 5.3.5.6 for additional discussion).

2) [[

]]

2.4.11 Technical Reviews (Oversight)

2.4.11.1 Technical Design Reviews

In addition, [[

]]

2.4.11.2 Software Development Process & Baseline Reviews

Section 4.4 describes in detail the process that was used to develop the CGS PRNMS firmware, including [[ ]]. Although this process was devised by GEH to establish a formal set of standards and procedures for NUMAC software products, following the process also results in assurance that the hardware design is correct and compatible with the software. There are at least two reasons. First, [[

]]

2.4.12 Design Verification

[[

]]

2.4.13 Testing

Multiple layers of testing are performed over the development life cycle to assure the quality of NUMAC equipment. A discussion of the dedication process that is applied to hardware items, as applicable, is provided in Section 2.4.8.

[[

]]

Finally, ENW and GEH tested the entire assembled PRNMS during FAT.

2.4.14 Programmable Logic Device Firmware Development

PLD firmware applied to the CGS PRNM project is discussed in Section 4.4. See Section 4.4 (4.4.6 through 4.4.7) for a discussion about PLD programming.

3. Software Architecture

3.1 Introduction

NEDC-33696P (Reference 4) is designed and structured to address the following Reference 15 items within the context of the integrated NUMAC PRNM System Architecture:

- System Description (D.1.2, D.9.2, D.10.2)
- Hardware Architecture Descriptions (D.1.2)
- Software Architecture Descriptions (D.3.2, D.4.4.3.2)
- Theory of Operations

3.2 Overview

The scope for the safety-related portions of the NUMAC PRNM System includes detailed examinations of the sub-systems, interfaces to non-safety sub-systems, and the hardware and software architectures within each sub-system. These examinations address timing, accuracy, mechanisms to address vulnerabilities, and response to faults, failures, and degraded conditions.

The scope for the non-safety-related portions of the NUMAC PRNM System is limited to the identification of sub-systems, interfaces, and examining aspects of hardware and software architectures for vulnerabilities which could potentially threaten, inhibit, or adversely affect the actuation of safety functions.

3.3 Regulatory Evaluation

The software architecture description is contained in the SRP, BTP 7-14 Section B.3.3.2, "Design Activities - Software Architecture Description." This section states that the Software Architecture Description should describe all of the functional and software development process characteristics listed, and that NUREG/CR-6101 (ADAMS Accession No. ML072750055), Section 3.3.1 "Hardware and Software Architecture," and Section 4.3.1, "Hardware/Software Architecture Specifications," contain relevant guidance.

3.4 Software Architecture Evaluation

NEDC-33696P (Reference 4) describes the System Architecture & Theory of Operations of NUMAC PRNM as specifically configured for CGS. Refer to NEDC-33696P (Reference 4) for the Software and Hardware Architecture descriptions.

4. Software Development Process

4.1 Introduction

This section describes the processes that were used to develop and test the CGS PRNMS microprocessor firmware, the degree of independence that existed during the project, and the compensatory measures to be taken in order to close gaps with respect to the degree of independence described in Institute of Electrical and Electronics Engineers (IEEE) Standard 1012-1998 (Reference 35). The discussion includes PLDs, including those cases where legacy PLDs are used, and also the limited cases where changes to legacy PLDs are necessary. The level of detail is consistent with information requirements in the ISG for the Licensing Process of Reference 15.

BTP 7-14 (Reference 36) contains the evaluation criteria for the high quality development process that is applicable to important to safety system programming, which includes the PRNMS. Where applicable, the Software Development Process identifies mapping of Reference 36 to development processes and products, including either information or mapping of the guidance to sections within the referenced documents. A detailed mapping to Reference 35 is also included.

4.2 Overview

Sections 4.4.1 through 4.4.4 describe the software planning documentation that was in place during the project, the implementation of the project, and software design outputs. Whenever independence is discussed in these sections, it refers to the degree of independence that was built-in to the GEH processes and existed during the project, but does not include the compensatory measures that are to be taken to close the gaps from IEEE Standard 1012-1998 (Reference 35). The information in Section 4.4 through 4.4.4 is similar to information under review by the NRC for the Grand Gulf Nuclear Station (GGNS) PRNM System Software Development Processes (Reference 37).

Sections 4.4.5 and 4.4.6 describe in more detail the independence that was built-in to the GEH processes while developing and validating microprocessor firmware and PLDs. The discussion in these sections also does not include the compensatory measures to be undertaken to close gaps from Reference 35. The information in Section 4.4.5 is similar to information under review by the NRC for the GGNS PRNM System Software Development Processes (Reference 37). The information in Section 4.4.6 is similar to information under review by the NRC for the GGNS PRNM System Software Development Processes (Reference 38).

Section 4.4.7 describes the method for Microprocessor Firmware and PLD identification. The information in Section 4.4.7 is similar to information under review by the NRC for the GGNS PRNM System Software Development Processes (Reference 39).

Section 4.4.8 provides a detailed mapping of the approach that was in place during the PRNMS project to Reference 35. [[

]] The information in Section 4.4.8 is similar to information under review by the NRC for the GGNS PRNMS Software Development Processes (Reference 40).

4.3 Regulatory Evaluation

The regulatory requirements applicable to digital I&C upgrades with respect to the software development process are:

10 CFR 50.55a(a)(1) addresses Quality Standards for Systems Important to Safety: "Structures, systems, and components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed."

10 CFR 50.55a(h)(3), "Safety Systems" incorporates IEEE Standard 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995 into the federal regulations by reference.

> Regulatory Guide 1.152, Revision 2, "Criteria for Use of computers in Safety Systems of Nuclear Power Plants," endorsed IEEE Standard 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Clause 5.3.1 of IEEE Standard 7-4.3.2, "Software Development," provides guidance. (See also Section D.10.4.4.2.3.1).

GDC 1, "Quality Standards and Records" states: "Structures, systems, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed..." SRP Branch Technical Position (BTP) 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems."

IEEE Standard 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes," as endorsed by Regulatory Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

IEEE Standard 1028-1997, "IEEE Standard for Software Reviews and Audits," as endorsed by Regulatory Guide 1.168 Revision 1, "Verification, Validation, Reviews, and Audits For Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

Regulatory Guide 1.168 Revision 1, "Verification, Validation, Reviews, and Audits For Digital Computer Software Used In Safety Systems of Nuclear Power Plants."

IEEE Standard 1012-1998, "IEEE Standard for Software Verification and Validation," as endorsed by Regulatory Guide 1.168 Revision 1, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

IEEE Standard 828-1990, "IEEE Standard for Configuration Management Plans," as endorsed by Regulatory Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

IEEE Standard 829-1983, "IEEE Standard for Software Test Documentation," as endorsed by Regulatory Guide 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

IEEE Standard 1008-1987, "IEEE Standard for Software Unit Testing," as endorsed by Regulatory Guide 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

4.4 NUMAC Software Development Process Evaluation

The NUMAC Software Development Program is presented as an alternative approach to the independent and comprehensive software-specific process model defined by BTP 7-14 (Reference 36). Combined with the compensatory measures described, the goals of References 35 and 36 are met. The information provided is of sufficient detail, consistent with the information requirements of Reference 15, to demonstrate that the NUMAC Software Development Program is a well-defined and disciplined process that results in a high quality product, suitable for use in safety-related applications at nuclear power plants.

4.4.1 Software Planning Documentation (DI&C ISG-06 D.4.4.1)

The twelve software plans, identified in Section B.2.1 of Reference 36, define a comprehensive, independent, and self-contained set of software-specific processes, procedures, activities, and controls, that constitute a stand-alone software development program found acceptable by the NRC for development of software products used in safety-related applications at nuclear power plants. The GEH NUMAC Software Development Program is an alternate approach to the program defined by Reference 36.

The three NUMAC software development plans (SDPs) listed below were first released in October 1990, nearly seven years prior to the initial release of BTP HICB 14 in June 1997, and more than sixteen years prior to the release of the current revision of BTP 7-14 in March 2007. The three NUMAC SDPs are:

- NUMAC Software Configuration Management Plan (SCMP, Reference 41)
- NUMAC Software Management Plan (SMP, Reference 42)
- NUMAC SVVP (Reference 34)

These plans and the software development life cycle processes that they represent have remained relatively unchanged since their initial release, except for minor changes to clarify and adjust to changing technology over the years. The current revisions of the three NUMAC software planning documents, as well as other life cycle products, are provided in Appendix A.

In contrast to BTP 7-14 (Reference 36), the NUMAC SDPs alone do not define a comprehensive, independent, and self-contained software development program. Instead, these plans define how software for NUMAC products is developed according to the policies and procedures that implement the GEH 10 CFR 50 Appendix B Quality Assurance program, NEDO-11209-04A, GE Nuclear Energy Quality Assurance Program Description (Reference 7), that has been reviewed and approved by the NRC.

The NUMAC Software Development Program comprises the following:

- The NUMAC SDPs listed above,
- The activities defined by GEH EOPs and CPs that implement the GEH QA program,
- The generic NUMAC (Product Line) Requirements Specification, and
- The GEH corporate configuration control tools and associated processes.

The evaluation of the NUMAC Software Development Program against the criteria of Reference 36 must include consideration of all these elements.

The following sections provide information consistent with the information requirements in Section D.4.4.1 of Reference 15 in order to enable the NRC staff to evaluate the NUMAC Software Development Program against the Reference 36 regulatory evaluation criteria for `software planning documentation. Table 4.4-1 below correlates the Reference 36 planning documents with the corresponding GEH project documents and applicable GEH policies and procedures.

Table 4.4-1 Mapping of BTP 7-14 Planning Documents to Applicable GEH Documents, Policies and Procedures

[[		
		]]

4.4.1.1 Software Management Plan (DI&C ISG-06 D.4.4.1.1)

The NUMAC SMP describes the process to be used for the design, development, and maintenance of NUMAC product software, which is closely aligned with the purpose of a SDP as defined by the criteria in BTP 7-14 (Reference 36). See the discussion below under Software Development Plan for details.

The PWP is the GEH document that addresses the project management aspects of the SMP as defined by the criteria in BTP 7-14 (Reference 36). The NUMAC SMP is used in conjunction with the PWP to address the SMP as defined by the criteria in BTP 7-14 (Reference 36).

Section 1.1 of the NUMAC SMP (Reference 42) states:

[[

]] The PWP fully addresses the topics discussed in IEEE Standard 1074-1995 (Reference 43), Clause 3.1.6, "Plan Project Management," as endorsed by Regulatory Guide (RG) 1.173 (Reference 44), as well as IEEE Standard 7-4.3.2-2003 (Reference 45) Clause 5.3.6, "Software Project Risk Management," as endorsed by RG 1.152 (Reference 46).

As stated in [[

]]

Project risk management is also a key function of the PWP. [[

]]

The CGS PRNM PWP also defines the interface between ENW (the licensee) and GEH (the vendor) for the development of the CGS PRNMS and discusses how ENW provides oversight of the software development program through reviews of project deliverables, audits, and participation in the FAT.

See the discussion under Software Quality Assurance Plan, below, for an explanation of the relationship between the software development group and the quality assurance function, including the independence aspects. Independence of the quality assurance function is also addressed in the Section 4.4.5, Built-in Organizational Independence that Existed during Development & Programming of Microprocessor Firmware.

See the discussion under Software Safety Plan, below, for an explanation of the relationship between the software development group and the software safety function, including the independence aspects. Independence of the software safety function is also addressed in Section 4.4.5.

See the discussion under Software V&V Plan, below, for an explanation of the relationship

between the software development group and the V&V function, including the independence aspects. Independence of the V&V function is also addressed in the Section 4.4.5. [[

]]

The CGS PRNM PWP identifies the project team, roles, and responsibilities. [[

]] See discussion under Software V&V Plan, below.

[[

]] These roles and responsibilities are explained in more detail throughout the remaining discussion in this section.

See the discussion in Section 11, Secure Development and Operational Environment (SDOE) Controls, for a description of the secure development and environment methods and controls.

4.4.1.2 Software Development Plan (DI&C ISG-06 D.4.4.1.2)

[[

]]

Together these three plans, used in conjunction with GEH policies and procedures, define software life cycle process activities that are consistent with both the development process activities and the associated integral process activities described in IEEE Standard 1074-1995 (Reference 43) as endorsed by RG 1.173 (Reference 44). Compliance with the specific guidance provided by IEEE Standard 7-4.3.2-2003, (Reference 45), Clause 5.3.1, "Software Development," as endorsed by RG 1.152 (Reference 46), is addressed under Software QA Plan (SQAP) in Section 4.4.1.3.

[[

]] It should be noted that commercial grade software and commercial grade computer hardware are not used to perform any safety function in the NUMAC PRNMS.

The NUMAC design philosophy is in accordance with the criterion from Reference 45, Clause 5.3.2, "Software Tools," as endorsed by Reference 46 that software tools should be used in a manner such that defects not detected by the software tools are detected by V&V activities. [[

]] Section 4.4.6, Microprocessor & PLD Firmware Development and Testing Tools, addresses the use of software tools in detail.

[[

]]

This document follows the guidance in NUREG/CR-6463 (Reference 50) with specific deviations noted and the rationale for these deviations explained.

4.4.1.3 Software QA Plan (DI&C ISG-06 D.4.4.1.3)

As described above, the NUMAC SCMP, SMP, and SVVP are designed to work in conjunction with the policies and procedures that implement the GEH 10 CFR 50 Appendix B compliant nuclear quality assurance program (Reference 7) developed in accordance with RG 1.28 (Reference 51). Reference 45," Clause 5.3.1, "Software Development" refers to IEEE Standard 730-1998 (Reference 52) for guidance on developing SQAPs. Likewise, References 43 and 53 refer to an earlier revision of this standard.

[[

]]

For example,

[[

]]

The procedures identified above are just a few examples of the GEH policies and procedures that implement the GEH QA program that also happen to address topics from Reference 52. All NUMAC software development work is conducted under the auspices of the GEH QA program.

[[

]]

4.4.1.4 Software Integration Plan (DI&C ISG-06 D.4.4.1.4)

[[

]] This phase of the design process fully addresses the topics discussed in Reference 43, Clause 5.3.7, "Plan Integration," as endorsed by RG 1.173 (Reference 44). [[

]]

4.4.1.5 Software Installation Plan (DI&C ISG-06 D.4.4.15)

Section D.4.4.1.5 of Reference 15 states:

The Software Installation Plan may not be reviewed in the staff SE. Application installation is not a part of the licensing process. The Software Installation Plan may be inspected as part of the regional inspection program. The licensee should be prepared to support any regional inspections of the installation prior to the system being put into operational use.

[[

]] a Software Installation Plan as described in Reference 36 is neither necessary nor applicable.

4.4.1.6 Software Maintenance Plan (DI&C ISG-06 D.4.4.1.6)

Section D.4.4.1.6 of Reference 15 states:

The Software Maintenance Plan may not be reviewed in the staff SE. Licensee maintenance is not a part of the licensing process. The Software Maintenance Plan may be inspected as part of the regional inspection program. The licensee should be prepared to support any regional inspections of the maintenance plan prior to the system being put into operational use.

[[

]] a Software Maintenance Plan as described in Reference 36 is neither necessary nor applicable.

4.4.1.7 Software Training Plan (DI&C-ISG-06 D.4.4.1.7)

Section D.4.4.1.7 of Reference 15 states:

The software training plan may not be reviewed in the staff SE. Licensee training is not a part of the licensing process. Instead, it falls under the regional inspection purview. The licensee should be prepared to support any regional inspections of the training done in preparation for use of the proposed system prior to the system being put into operational use.

Training on PRNMS is handled through normal plant training processes and procedures; therefore, a Software Training Plan as described in Reference 36 is neither necessary nor applicable.

4.4.1.8 Software Operations Plan (DI&C-ISG-06 D.4.4.1.8)

Section D.4.4.1.8 of Reference 15 states:

The Software Operations Plan may not be reviewed in the staff SE. Licensee operations are not a part of the licensing process. The Software Operations Plan may be inspected as part of the regional inspection program. The licensee should be prepared to support any regional inspections of the preparation for use of the proposed system prior to the system being put into operational use.

Operation of PRNMS is controlled by plant operating procedures; therefore, a SOP as described in Reference 36 is neither necessary nor applicable.

4.4.1.9 Software Safety Plan (DI&C-ISG-06 D.4.4.1.9)

[[

]] This provides a comparable level of assurance to that which would be achieved by compliance with Reference 36 criteria for software safety analysis. See Sections 4.4.2.1 and 4.4.5 for further details on software safety analysis.

4.4.1.10 Software V&V Plan DI&C ISG-06 D.4.4.1.10)

The NUMAC SVVP is used in conjunction with GEH procedures that govern design verification activities to establish methods for V&V that are largely consistent with guidance provided in Reference 35 as endorsed by RG 1.168 (Reference 57). The NUMAC Software Development Program V&V activities are also consistent with guidance found in Reference 45, Clause 5.3.3, "Verification and Validation," as endorsed by Reference 46, as well as Reference 46, Section C.2.2.1, "System Features." Reference 34 used in conjunction with standard GEH procedures as described below defines V&V activities for NUMAC software that are comparable to those described in the regulatory guidance and are consistent with the objectives stated in the regulatory guidance.

[[

]] Additional compensatory measures, to ensure an acceptable level of IV&V for the CGS project software, are described in Section 4.4.8.

[[

]]

The discussion above and in Section 4.4.5 describe the V&V organization and independence aspects. Additional compensatory measures, to ensure an acceptable level of IV&V for the CGS project software, are described in Section 4.4.8. [[

]]

4.4.1.11 Software Configuration Management Plan (DI&C ISG-06 D.4.4.1.11)

The NUMAC SCMP is used in conjunction with GEH procedures that implement the GEH corporate configuration management system to establish a software configuration management program for NUMAC products that is consistent with guidance provided in Reference 43, Clause 7.2.4, "Plan Configuration Management," as endorsed by RG 1.173 (Reference 44) as well as guidance provided in IEEE Standard 828 (Reference 58), as endorsed by RG 1.169 (Reference 59). The NUMAC SCMP (Reference 41) used in conjunction with GEH procedures is also consistent with guidance provided in (Reference 45), Clause 5.3.5, "Software configuration management." [[

]] Reference 41 used in

conjunction with standard GEH procedures as described below provides for comparable configuration management of NUMAC software that is consistent with the objectives stated in the regulatory guidance, even though the NUMAC SCMP does not conform to the conventional model of a Software Configuration Management Plan as described in References 53 and 58.

[[

]]

4.4.1.12 Software Test Plan (DI&C SISG-06 D.4.4.1.12)

The NUMAC SVVP defines multiple layers of testing to be performed over the software development life cycle defined by the NUMAC SMP in order to assure the quality of NUMAC software:

[[

]] IEEE Standard 829 (Reference 60) as endorsed by RG 1.170 (Reference 61) as wells as IEEE Standard 1008-1987 (Reference 62), as endorsed by RG 1.171 (Reference 63), [[

]] See the discussions of Module Test Report and Integration Test Report under Testing Activities, below, for additional information.

[[

]] Reference 35, as endorsed by Reference 57. [[

]]

See the discussion above under Software V&V Plan, as well as the discussion in Section 4.4.5, for further details regarding the degree of independence provided at various stages of the NUMAC software development process for all V&V activities. Additional compensatory measures, to ensure an acceptable level of IV&V for the CGS project software, are described in Section 4.4.8.

4.4.2 Software Plan Implementation (DI&C ISG-06 D.4.4.2)

The following sections provide information that is intended to be consistent with the information requirements in Section D.4.4.2 of Reference 15 in order to enable the NRC staff to evaluate the NUMAC Software Development Program against the BTP 7-14 (Reference 36) regulatory evaluation criteria for software implementation activities. Table 4.4-2 below correlates the Reference 36 software plan implementation activities with the corresponding GEH activities and associated documentation.

Table 4.4-2 Correlation of BTP 7-14 Software Plan Implementation Activities to GEH Implementation Activities and Documentation

[[		]]

4.4.2.1 Software Safety Analysis

As previously stated, the NUMAC Software Development Program includes elements that sufficiently address software safety, [[

]] These records are maintained in the PDMS where they are available for review by the NRC staff at the GEH office.

4.4.2.2 V&V Analysis and Reports (DI&C ISG-06 D.4.4.2.2)

[[

]]

The V&V records for all baseline configuration items, as well as the baseline review records that show that verification tasks were successfully accomplished at each design phase in the life cycle, are maintained in the PDMS where they are available for review by the NRC staff at the GEH office.

4.4.2.3 Configuration Management Activities (DI&C ISG-06 D.4.4.2.3)

The PDMS is the primary configuration management tool for all engineering controlled documentation, including software for NUMAC products.

[[

]]

The PDMS provides unique identification of each configurable item by document identification number, title, and revision. [[

]] Revision history of all baseline configuration items is tracked and reported by the PDMS.

[[

]]

The configuration management records for all baseline configuration items, as well as the baseline review records that establish and document the configuration at each design phase in the life cycle, are maintained in the PDMS where they are available for review by the NRC staff at the GEH office.

4.4.2.4 Testing Activities (DI&C ISG-06 D.4.4.2.4)

[[

]]

The module test reports, integration test reports, validation test procedures, validation test procedure traceability matrices, validation test reports, and documented acceptance of the FAT results are maintained in the PDMS where they are available for review by the NRC staff at the GEH office.

4.4.3 Design Outputs (DI&C ISG-06 D.4.4.3)

The following sections provide information that is intended to be consistent with the information requirements in Section D.4.4.3 of Reference 15 in order to enable the NRC staff to evaluate the NUMAC Software Development Program against the Reference 36 regulatory evaluation criteria for software life cycle design outputs. Table 4.4-3 below correlates the Reference 36 design outputs with the corresponding GEH NUMAC software development process design outputs.

Table 4.4-3 Correlation of BTP 7-14 Design Outputs to GEH NUMAC Design Outputs

[[	
	]]

4.4.3.1 Software Requirements Specification (DI&C ISG-06 D.4.4.3.1)

[[

]]

References 5 and 48 are provided in Appendix A. These and other documents that comprise the Definition and Planning baseline are maintained in the PDMS. Documents referenced within the system requirements specification listed above and other documents from the Definition and Planning baseline not provided with this submittal are available for review by the NRC staff at the GEH office.

[[

]]

These documents are provided in Appendix A. These and other documents that comprise the Product Performance Definition baseline are maintained in the PDMS. Documents referenced within the specifications listed above and other documents from the Product Performance Definition baseline not provided with this submittal are available for review by the NRC staff at the GEH office.

These documents establish the software requirements similar to a conventional Software Requirements Specification as described in IEEE Standard 830 (Reference 66), as endorsed by RG 1.172 (Reference 67).

4.4.3.2 Software Architecture Description (DI&C ISG-06 D.4.4.3.2)

[[

]] These requirements and the details of the software architecture are further refined in the instrument specific software design specifications established during the High Level Software Design phase.

Reference 47 is provided in Appendix A.

Additionally, refer to Section 3, Software Architecture Description, for the PRNMS software architecture description.

4.4.3.3 Software Design Specification (DI&C ISG-06 D.4.4.3.3)

[[

]]

References 68 and 69 are provided in Appendix A. These documents and other documents that comprise the High Level Software Design baseline are maintained in the PDMS. The documents referenced within the specifications listed above and other documents from the High Level Software Design baseline not provided with this submittal are available for review by the NRC staff at the GEH office.

4.4.3.4 Code Listings (DI&C ISG-06 D.4.4.3.4)

[[

]] Source code listings are maintained in the PDMS where they are available for review by the NRC staff at the GEH office.

4.4.3.5 System Build Documents (DI&C ISG-06 D.4.4.3.5)

[[

]]

The FRDs and firmware drawings are maintained in the PDMS where they are available for review by the NRC staff at the GEH office.

4.4.3.6 Installation Configuration Tables (DI&C ISG-06 D.4.4.3.6)

Section D.4.4.3.6 of Reference 15 states:

> The Installation Configuration Tables should not be reviewed in the staff SE. Licensee operations are not a part of the licensing process, but they may be inspected as part of the regional inspection program. The licensee should be prepared to support any regional inspections of the preparation for use of the proposed system prior to the system being put into operational use.

[[

]] Determination of cycle-specific parameter values is not within the scope of the NUMAC Software Development Program.

4.4.3.7 Operations Manuals (DI&C ISG-06 D.4.4.3.7)

Section D.4.4.3.7 of Reference 15 states:

> The Operations Manual should not be reviewed in the staff SE. Licensee operations are not a part of the licensing process. The Operations Manual may be inspected as part of the regional inspection program. The licensee should be prepared to support any regional inspections of the preparation for use of the proposed system prior to the system being put into operational use.

[[

]]

4.4.3.8 Software Maintenance Manuals (DI&C ISG-06 D.4.4.3.8)

Section D.4.4.3.8 of Reference 15 states:

> The Software Maintenance Manuals should not be reviewed in the staff SE. Licensee maintenance is not a part of the licensing process, they may be inspected as part of the regional inspection program. The licensee should be prepared to support any regional inspections of the preparation for use of the proposed system prior to the system being put into operational use.

[[

]]

4.4.3.9 Software Training Manuals (DI&C ISG-06 D.4.4.3.9)

Section D.4.4.3.9 of Reference 15 states:

> The Software Training Manuals should not be reviewed in the staff SE. Licensee training is not a part of the licensing process, they may be inspected as part of the

regional inspection program. The licensee should be prepared to support any regional inspections of the preparation for use of the proposed system prior to the system being put into operational use.

[[

]]

4.4.4 Conclusion (Sections 4.4.1, 4.4.2, and 4.4.3)

The GEH NUMAC Software Development Program used for the CGS PRNM project is an alternative approach to the independent and comprehensive software-specific process model defined by BTP 7-14 (Reference 36). This alternate approach addresses all critical aspects of a high quality development process and provides a level of quality assurance comparable to that which would be achieved by compliance with Reference 36. The GEH NUMAC Software Development Program, although different from the program described in Reference 36, is a well-defined and disciplined process that results in a high quality product, suitable for use in safety-related applications at nuclear power plants, such as the NUMAC PRNMS for CGS.

4.4.5 Built-in Organizational Independence that Existed during Development & Programming of Microprocessor Firmware

BTP 7-14 (Reference 36) identifies that the SMP "should ensure that the quality assurance organization, the software safety organization and the software V&V organization maintain independence from the development organization. In particular, the plan should ensure that these assurance organizations do not report to the development organization, and not be subject to the financial control of the development organization."

Overview

The information in Section 4.4.5 is similar to information under review by the NRC for the GGNS PRNM System Software Development Processes (Reference 37).

The Software Development Process, described in Section 4.4, includes characteristics to address independence of microprocessor firmware development.

4.4.5.1 Microprocessor Firmware Development

The NUMAC SMP, NUMAC SCMP, and NUMAC SVVP provide the procedure and process requirements for software development and delivery activities. These are in addition to GEH policies and procedures developed in accordance with 10 CFR 50 Appendix B requirements for independent design verification, technical reviews, quality assurance, and other engineering activities. A combination of organizational independence, independent design verifications, baseline reviews, and technical design reviews provides assurance that the design has adequate quality, safety, reliability, and performance.

[[

]]

This portion of the discussion is provided in two sections. Section 4.4.5.2 provides information that is not baseline-specific. Section 4.4.5.3 provides baseline-specific information.

4.4.5.2 Generic Across Baselines

4.4.5.2.1 GEH Organizational Structure for PRNMS

Figure 4.4-1 describes the organizations involved in the PRNMS project.

4.4.5.2.2 Project Management Organization

[[

]]

4.4.5.2.3 Quality Assurance (QA) Organization

[[

]]

4.4.5.2.4 Chief Engineer's Office

[[ ]]

4.4.5.2.5 Services I&C Engineering Organization

[[

]]

4.4.5.2.5.1 The I&C Applications Engineering organization has responsibilities to:

(a) [[

]]

4.4.5.2.5.2 The I&C Technology organization has responsibilities to:

(a) [[

]]

4.4.5.2.6 Organizational Independence

[[

]]

[[

]]

Figure 4.4-1 Simplified Outline of GEH Organizational Structure

4.4.5.2.7 Design Verification

The requirements for GEH design verification are defined in GEH policies and procedures and comply with the requirements in 10 CFR 50 Appendix B. Independent design verification is a key process in GEH software development. The NUMAC SVVP (Reference 34), Section 2.2, states the following:

[[

]]

References 34 and 42 specify various requirements for independent design verification. The GEH design process requires independent design verification at various stages of the design.

All design verifications, including verification by an individual within the same organization, must abide by the following independence requirements for the RV. Reference 29, Section 7.1.3, states that the following independence criteria shall be met.

[[

]]

4.4.5.2.8 Baseline Review Process

Reference 42 defines the deliverables for each life-cycle baseline. A Baseline Review is performed at the conclusion of each life-cycle baseline to provide a formal, independent evaluation of conformance to the design process, effectiveness, and completeness of the process to that point. [[

]]

4.4.5.2.9 Technical Design Review Process

GEH policies and procedures also require periodic Technical Design Reviews be conducted for each project. For the CGS PRNMS project there are three design reviews performed and documented at various stages of the project in accordance with GEH policies and procedures. Design review objectives include verifying that the design meets all design requirements, including safety requirements. The Design Review also ensures product operability, safety and reliability. [[

]]

4.4.5.2.10 Items Having Safety-Significant Aspects

For the CGS PRNMS project, the basis for identifying an item as having safety-significant aspects is outlined in Reference 1. This basis is used to identify safety-significant aspects in life cycle baseline documentation. [[

]]

4.4.5.2.11 Safety-Significance Determinations Equivalency to Software Safety Planning

Safety-significant aspects of the design are identified in the baseline documentation described in Section 4.4.5.3, Baseline Specific Information, below. This is compliant with the BTP 7-14 (Reference 36) requirement that *appropriate safety requirements be included in the software requirements specification.*

Identifying the safety-significant aspects in the baseline documentation provides assurance that safety-significant aspects are sufficiently addressed during the independent design verification.

[[

]] For the PRNMS project, CCFs are addressed in Section 6, Defense-in-Depth & Diversity.

4.4.5.2.12 Summary of Generic Baselines Information

The NUMAC SMP, NUMAC SCMP, NUMAC SVVP, and GEH policies and procedures provide multiple layers of design verifications, independent baseline reviews, independent technical design reviews, and QA confirmation to ensure that the design has adequate quality, safety, reliability, and performance of the software product. Organizational and financial independence is provided at various stages of the software design process as defined in these procedures. The application of these processes in each baseline is described in the next section below.

4.4.5.3 Baseline Specific Information

4.4.5.3.1 Baseline 1 Definition and Planning Phase

4.4.5.3.1.1 Scope/Coverage of V&V

[[

]]

4.4.5.3.1.2 Items Having Safety-Significant Aspects

[[

]]

4.4.5.3.1.3 Safety-Significance Determinations Equivalency to Software Safety Planning

[[

]]

4.4.5.3.2 Baseline 2 Product Performance Definition Phase

4.4.5.3.2.1 Scope/Coverage of V&V

[[

]]

4.4.5.3.2.2 Items Having Safety-Significant Aspects

[[

]]

4.4.5.3.2.3 Safety-Significance Determinations Equivalency to Software Safety Planning

[[

]]

4.4.5.3.3 Baseline 3 High Level Software Design Phase

4.4.5.3.3.1 Scope/Coverage of V&V

[[

]]

4.4.5.3.3.2 Items Having Safety-Significant Aspects

[[

]]

4.4.5.3.3.3 Safety-Significance Determinations Equivalency to Software Safety Planning

[[

]]

4.4.5.3.4 Baseline 4 Detailed Design/Code/Module Test Phase

4.4.5.3.4.1 Scope/Coverage of V&V

[[

]]

4.4.5.3.4.2 Items Having Safety-Significant Aspects

[[

]]

4.4.5.3.4.3 Safety-Significance Determinations Equivalency to Software Safety Planning

[[

]]

4.4.5.3.5 Baseline 5 Integration Test Phase

4.4.5.3.5.1 Scope/Coverage of V&V

[[

]]

4.4.5.3.5.2 Items Having Safety-Significant Aspects

[[

]]

4.4.5.3.5.3 Safety-Significance Determinations Equivalency to Software Safety Planning

[[

]]

Section 4.4.8 provides a detailed mapping of the approach to software V&V for the PRNMS safety-related firmware to the V&V activities per IEEE Standard 1012 (Reference 35). [[

]]

4.4.5.3.6 Baseline 6 Validation and Firmware Issue Phase

4.4.5.3.6.1 Scope/Coverage of V&V

[[

]]

4.4.5.3.6.2 Items Having Safety-Significant Aspects

[[

]]

4.4.5.3.6.3 Safety-Significance Determinations Equivalency to Software Safety Planning

[[

]]

4.4.6 Microprocessor & PLD Firmware Development and Testing Tools

BTP 7-14 (Reference 36) identifies that the SDP "should require that tools be qualified with a degree of rigor and level of detail appropriate to the safety significance of the software that is developed using the tools. Methods, techniques and tools that produce results that cannot be verified or that are not compatible with safety requirements should be prohibited, unless analysis shows that the alternative would be less safe."

Overview

The information in Section 4.4.6 is similar to information under review by the NRC for the GGNS PRNM System Software Development Processes (ADAMS Accession

No. ML111370259).

The use of V&V activities to confirm the acceptability of software tools is one of the accepted methods in References 15 and 45, and meets the criteria of Reference 36, Section B.3.1.2.3. This section addresses three focus areas to demonstrate that the GEH process for software tools meets the listed requirements for tool qualification as specified in Reference 15, Section D.10.4.2.3.2; Reference 45, Clause 5.3.2; and Reference 36, Section B.3.1.2.3.

4.4.6.1 Legacy Programmable Logic Device (PLD) Firmware Development

Most of the PLD firmware applied to the CGS PRNM project is from previously released (legacy) designs. Programmable logic (PL) changes will be performed in accordance with the NUMAC software development program, along with the compensatory measures described in Section 4.4.8. [[

]] The remainder of this section provides a discussion of the development of legacy PLD firmware applied to the CGS PRNM project.

The legacy PLD firmware follows a hardware process compliant to GEH policies and procedures and in compliance with 10 CFR 50 Appendix B.

[[

]]

4.4.6.2 V&V Activities

[[

]]

4.4.6.3 Development and Production Tools

The use of V&V activities to confirm the acceptability of the software tools is one of the accepted methods in References 15 and 45, and meets the criteria of Reference 36, Section B.3.1.2.3.

[[

]]

NUMAC firmware designed for microprocessor and PLD devices utilize a suite of Original Equipment Manufacturer (OEM) development and production tools supplied by vendors from GEH's Qualified Suppliers List who, in many cases, are the same vendors/manufacturers that provide the devices used. Reference 45, Clause 5.3.2 allows the use of operational history to provide additional confidence of the suitability of the tools. Firmware developed using these

tools has been in service for 26 years in safety-related digital instrumentation deployed in nuclear power plants throughout the world. [[

]]

Table 4.4-4 provides the development and production tools used for CGS NUMAC PRNM firmware.

Table 4.4-4 CGS NUMAC PRNM Firmware Development and Production Tools

[[		
		]]

4.4.6.4 Conclusion

The application of GEH procedures and the NUMAC SDPs ensures the management of software tools used to develop and program NUMAC microprocessor and PLD firmware is in compliance with requirements for tool qualification listed in Reference 36 Section B.3.1.2.3, Reference 15 Section D.10.4.2.3.2, and Reference 45 Clause 5.3.2. Mandated V&V activities verify all results produced by software tools used to ensure any defects that may be introduced by them are detected.

4.4.7 Development & Programming of Microprocessor & PLD Firmware-Identification

Regulatory Guide 1.152 (Reference 46) endorses Reference 45, and Reference 45, Clause 5.11 states that "Means shall be included in the software such that the identification may be retrieved from the firmware using software maintenance tools."

Overview

The information in Section 4.4.7 is similar to information under review by the NRC for the GGNS PRNM System Software Development Processes (Reference 39).

The NUMAC SCMP specifies revision (including version) controls on an instrument, project, and firmware release basis. The PRNM software is released as hardware with an issued part number for identification.

Any changes in the software, either revision or version, would be released with a new part number. Therefore, the retrieval of the software identification can be accomplished without the use of software maintenance tools.

4.4.7.1 Microprocessor and PLD Firmware Identification

For each instrument application, the firmware programming is burned onto the EPROM or PLD that can only be changed or altered by GEH. The EPROM and PLD are treated as a hardware assembly with the firmware as one of its parts. An assembly part number is assigned to each EPROM or PLD. The assembly parts list includes the blank EPROM or PLD and the document for the software programming that includes the software or location where the software is archived and the checksum for the software. The checksum is used to confirm the correct software is burned into the EPROM or PLD. A label of the part number is then placed on the EPROM or PLD for the unique identification of the corresponding firmware. Both firmware and software are maintained in the GEH product management system as an issued part with configuration control.

As an issued part, the firmware is also maintained in the GEH quality system and can be retrieved without the need for any tools. The issuance of the part number is performed in accordance with the GEH EOPs. Compliance with Reference 45, Clause 5.11 is discussed below, based on the requirements of NUREG-0800 (Reference 70), Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Standard 7-4.3.2." In the discussion, each requirement is followed by an explanation of how it is met.

4.4.7.1.1 Appendix 7.1-D of NUREG-0800

Appendix 7.1-D of Reference 70, Section 5.11 Identification (IEEE Standard 7-4.3.2-2003 Clause 5.11), states:

> To provide assurance that the required computer system hardware and software are installed in the appropriate system configuration, the following identification requirements specific to software systems should be met:
>
> i. Firmware and software identification should be used to assure the correct software is installed in the correct hardware component.

ii. Means should be included in the software such that the identification may be retrieved from the firmware using software maintenance tools.

iii. Physical identification requirements of the digital computer system hardware shall be in accordance with the identification requirements in IEEE Standard 603-1991 (Reference 71).

iv. The identification should be clear and unambiguous. The identification should include the revision level, and should be traceable to configuration control documentation that identifies the changes made by that revision.

Item i: This requirement is met by the issuance of a part number for the firmware and by placing the part number label on the EPROM or PLD. The part number identifies both the type of IC being used and the software that is embedded into the EPROM or PLD.

Item ii: NUMAC firmware/software does not require the use of software maintenance tools like a PLC based system for maintenance. It is maintained within GEH quality system and can be retrieved as needed based on the issued part number. Any changes in the software would result in the issuance of a new part number.

Item iii: This requirement is met by the issuance of a part number for the firmware and by placing the part number label on the EPROM or PLD.

Item iv: This requirement is met in that each EPROM or PLD has a unique part number. Any revision or version change of the software would result in a change in the part number.

4.4.7.1.2 EPROM Identification

An example of the EPROM identification is as follows: The ASP EPROM is identified as 148C6123G00x. The parts list for 148C6123G00x would identify the EPROM assembly 265A3025G00x, where the group numbers are determined by the project application. The parts list for 265A3025 specifies the IC for the EPROM as 265A1404P004 and the software programming as 265A3028P001 for Group 1 application. The same structure applies to the identification of a PLD.

4.4.8 CGS PRNMS Software V&V Process & IEEE 1012-1998 Requirements

Introduction

RG 1.168 (Reference 57), Position 1 "Critical Software" states, in part, that: "Software used in nuclear power plant safety systems should be assigned integrity level 4 or equivalent, as demonstrated by a mapping between the applicant or licensee approach and integrity level 4 as defined in IEEE Standard 1012-1998."

Overview

The information in Sections 4.4.8 is similar to information under review by the NRC for the GGNS PRNM System Software Development Processes (Reference 40).

This section provides a detailed mapping of the approach to software V&V for the PRNMS

safety-related firmware versus the V&V activities per Reference 35 software integrity level 4 and describes compensatory measures to close gaps. This mapping demonstrates that V&V for software integrity level 4, as defined in Reference 35, and endorsed by Reference 57, is satisfied by the CGS PRNMS development process combined with the compensatory measures identified.

4.4.8.1 Table 4.4-5, Comparison of IEEE Standard 1012-1998 and GEH Software V&V Process for CGS PRNMS

Table 4.4-5 provides the overall approach of the GEH software V&V process and compares it with the overall requirements of Reference 35.

The first column shows the V&V process as outlined in Reference 35. Each design task is performed by a design team. An IV&V team will perform the V&V as specified in the V&V plan. Management review and approval of the V&V results is then performed.

[[

]]

4.4.8.2 Detailed Mapping of GEH Software V&V Process versus IEEE-1012-1998 V&V Tasks

[[

]]

4.4.8.3 Mapping of RG 1.168 Position 7

[[

]]

4.4.8.4 Conclusion

As shown in Table 4.4-5, [[

]]

Table 4.4-5 Comparison of IEEE Standard 1012-1998 and GEH Software V&V Process for CGS PRNMS

IEEE 1012 Requirement	GEH Process Requirements	Comments
Design Task Performed by Design Team	• [[	
V&V Task performed by IV&V Team		
Management Review and Approve of V&V Results		]]

Table 4.4-6 Detailed Mapping of GEH Software V&V Process versus IEEE Standard 1012-1998 V&V Tasks

V&V Task	Required Outputs	GEH Process	GEH Outputs	Comments
5.1.1 Management of V&V Activity (in parallel with all processes)				
(1) SVVP Generation. Generate an SVVP for all life cycle processes. The SVVP may require updating throughout the life cycle. Outputs of other activities are inputs to the SVVP. Establish a baseline SVVP prior to the Requirements V&V activities. Identify project milestones in the SVVP. Schedule V&V tasks to support project management reviews and technical reviews.	SVVP and Updates	[[		
(2) Baseline Change Assessment. Evaluate proposed software changes (e.g., anomaly corrections and requirement changes) for effects on previously completed V&V tasks. Plan iteration of affected tasks or initiate new tasks to address software baseline changes or iterative development processes. Verify and validate that the change is consistent with system requirements and does not adversely affect requirements directly or indirectly. An adverse effect is a change that could create new system hazards and risks or affect previously resolved hazards and risks.	Updated SVVP Task Report(s) — Baseline Change Assessment Anomaly Report(s)			
(3) Management Review of V&V. Review and summarize the V&V effort to define changes to V&V tasks or to redirect the V&V effort.	Updated SVVP Task Report(s) — Recommendations V&V Activity Summary Reports Recommendations to the V&V Final Report			

V&V Task	Required Outputs	GEH Process	GEH Outputs	Comments
Recommend whether to proceed to the next set of V&V and development life cycle activities, and provide task reports, anomaly reports, and V&V Activity Summary Reports to the organizations identified in the SVVP.				
Verify that all V&V tasks comply with task requirements defined in the SVVP.				
Verify that V&V task results have a basis of evidence supporting the results.				
Assess all V&V results and provide recommendations for program acceptance and certification as input to the V&V Final Report. The management review of V&V may use any review methodology such as provided in IEEE Standard 1028-1988 [B8].				
(4) Management and Technical Review Support. Support project management reviews and technical reviews (e.g., Preliminary Design Review, and Critical Design Review) by assessing the review materials, attending the reviews, and providing task reports and anomaly reports. Verify the timely delivery according to the approved schedule of all software products and documents. The management and technical review support may use any review methodology such as provided in IEEE Standard 1028-1988 [B8].	Task Report(s) — Review Results Anomaly Report(s)			
(5) Interface With Organizational and Supporting Processes. Coordinate the V&V effort with organizational (e.g., management, improvement) and supporting processes (e.g., quality assurance, joint review, and problem resolution). Identify the V&V data to be exchanged with these processes. Document the data exchange requirements in the SVVP.	Updated SVVP			]]

V&V Task	Required Outputs	GEH Process	GEH Outputs	Comments
5.2.1 Acquisition Support V&V Activity (acquisition process)				
(1) Scoping the V&V Effort. Define the project V&V software criticality (e.g., safety, security, mission critical, technical complexity). Assign a software integrity level to the system and the software. Establish the degree of independence (see Annex C), if any, required for the V&V. Provide an estimate of the V&V budget, including test facilities and tools as required. To scope the V&V effort, the following steps shall be performed: (a) Adopt the system integrity scheme assigned to the project. If no system integrity level scheme exists, then one is selected. (b) Determine the minimum V&V tasks for the software integrity level using Table 2 and the selected software integrity level scheme. (c) Augment the minimum V&V tasks with optional V&V tasks, as necessary. (d) Establish the scope of the V&V from the description of V&V tasks, inputs, and outputs defined in Table 1.	Updated SVVP	[[		
(2) Planning the Interface Between the V&V Effort and Supplier. Plan the V&V schedule for each V&V task. Identify the preliminary list of development processes and products to be evaluated by the V&V processes. Describe V&V access rights to proprietary and classified information. It is recommended that the plan be coordinated with the acquirer. Incorporate the project software integrity level scheme into the planning process.	Updated SVVP			
(3) System Requirements Review. Review the system requirements (e.g., system requirements specification, feasibility study report, business rules description) in the RFP or tender to: (1) verify the consistency of requirements to user needs, (2) validate whether the requirements can be satisfied by defined technologies, methods, and algorithms defined for the project (feasibility), and (3) verify whether objective information that can be demonstrated by testing is provided in the requirements (testability). Review other	Task Report(s) — System Requirements Review Anomaly Report(s)			]]

V&V Task	Required Outputs	GEH Process	GEH Outputs	Comments
requirements such as deliverable definitions, listing of appropriate compliance standards and regulations, user needs, etc., for completeness, correctness, and accuracy.				
5.3.1 Planning V&V Activity (supply process)				
(1) Planning the Interface Between the V&V Effort and Supplier. Review the supplier development plans and schedules to coordinate the V&V effort with development activities. Establish procedures to exchange V&V data and results with the development effort. It is recommended that the plan be coordinated with the acquirer. Incorporate the project software integrity level scheme into the planning process.	Updated SVVP	[[		
(2) Contract Verification. Verify that (1) system requirements (from RFP or tender, and contract) satisfy and are consistent with user needs; (2) procedures are documented for managing requirement changes and for identifying the management hierarchy to address problems; (3) procedures for interface and cooperation among the parties are documented, including ownership, warranty, copyright, and confidentiality; and (4) acceptance criteria and procedures are documented in accordance with requirements.	Updated SVVP Task Report(s) — Contract Verification Anomaly Report(s)			]]
5.4.1 Concept V&V Activity (developing process)				
(1) Concept Documentation Evaluation. Verify that the concept documentation satisfies user needs and is consistent with acquisition needs. Validate constraints of interfacing systems and constraints or limitations of proposed approach. Analyze system requirements and validate that the following satisfy user needs: (1) system functions; (2) end-to-end system performance; (3) feasibility and testability of the functional requirements; (4) system architecture design; (5) operation and maintenance requirements; and (6) migration requirements from an existing system where applicable.	Task Report(s) – Concept Documentation Evaluation Anomaly Reports	[[		

V&V Task	Required Outputs	GEH Process	GEH Outputs	Comments
(2) Criticality Analysis. Determine whether software integrity levels are established for requirements, detailed functions, software modules, subsystem, or other software partitions. Verify that the assigned software integrity levels are correct. If software integrity levels are not assigned, then assign software integrity levels to the system requirements. Document the software integrity level assigned to individual software components (e.g., requirements, detailed functions, software modules, subsystems, or other software partitions). For V&V planning purposes, the most critical software integrity level assigned to individual elements shall be the integrity level assigned to the entire software. Verify whether any software component can influence individual software components assigned a higher software integrity level, and if such conditions exist, then assign that software component the same higher software integrity level.	Task Report(s) – Software Integrity Levels Task Report(s) – Criticality Analysis Anomaly Report(s)			
(3) Hardware/Software/User Requirements Allocation Analysis. Verify the correctness, accuracy, and completeness of the concept requirement allocation to hardware, software, and user interfaces against user needs. (3.1) Correctness a. Verify that performance requirements (e.g., timing, response time, and throughput) allocated to hardware, software, and user interfaces satisfy user needs. (3.2) Accuracy a. Verify that the internal and external interfaces specify the data formats, interface protocols, frequency of data exchange at each interface, and other key performance requirements to demonstrate compliance with user requirements. (3.3) Completeness a. Verify that application specific requirements such as functional diversity, fault detection, fault isolation, and diagnostic and error recovery satisfy user needs.	Task Report(s) — Hardware/ Software/User Requirements Allocation Analysis Anomaly Report(s)			

V&V Task	Required Outputs	GEH Process	GEH Outputs	Comments
b. Verify that the user's maintenance requirements for the system are completely specified. c. Verify that the migration from the existing system and replacement of the system satisfy user needs.				
(4) Traceability Analysis. Identify all system requirements that will be implemented completely or partially by software. Verify that these system requirements are traceable to acquisition needs. Start the software requirements traceability analysis with system requirements.	Task Report(s) — Traceability Analysis Anomaly Report(s)			
(5) Hazard Analysis. Analyze the potential hazards to and from the conceptual system. The analysis shall: (1) identify the potential system hazards; (2) assess the severity of each hazard; (3) assess the probability of each hazard; and (4) identify mitigation strategies for each hazard.	Task Report(s) — Hazard Analysis Anomaly Report(s)			
(6) Risk Analysis. Identify the technical and management risks. Provide recommendations to eliminate, reduce, or mitigate the risks.	Task Report(s) — Risk Analysis Anomaly Report(s)			]]
5.4.2 Requirements V&V Activity (development process)				
(1) Traceability Analysis. Trace the software requirements (SRS and IRS) to system requirements (Concept Documentation), and system requirements to the software requirements. Analyze identified relationships for correctness, consistency, completeness, and accuracy. The task criteria are as follows: (1.1) Correctness a. Validate that the relationships between each software requirement and its system requirement are correct. (1.2) Consistency a. Verify that the relationships between the software and system requirements are specified to a consistent level of detail. (1.3) Completeness a. Verify that every software requirement is traceable to a system requirement with sufficient detail to show	Task Report(s) — Traceability Analysis Anomaly Report(s)	[[		

V&V Task	Required Outputs	GEH Process	GEH Outputs	Comments
compliance with the system requirement. b. Verify that all system requirements related to software are traceable to software requirements. (1.4) Accuracy a. Validate that the system performance and operating characteristics are accurately specified by the traced software requirements.				
(2) Software Requirements Evaluation. Evaluate the requirements (e.g., functional, capability, interface, qualification, safety, security, human factors, data definitions, user documentation, installation and acceptance, user operation, and user maintenance) of the SRS and IRS for correctness, consistency, completeness, accuracy, readability, and testability. The task criteria are as follows: (2.1) Correctness a. Verify and validate that the software requirements satisfy the system requirements allocated to software within the assumptions and constraints of the system. b. Verify that the software requirements comply with standards, references, regulations, policies, physical laws, and business rules. c. Validate the sequences of states and state changes using logic and data flows coupled with domain expertise, prototyping results, engineering principles, or other basis. d. Validate that the flow of data and control satisfy functionality and performance requirements. e. Validate data usage and format. (2.2) Consistency a. Verify that all terms and concepts are documented consistently. b. Verify that the function interactions and	Task Report(s) — Software Requirements Evaluation Anomaly Report(s)			

V&V Task	Required Outputs	GEH Process	GEH Outputs	Comments
assumptions are consistent and satisfy system requirements and acquisition needs. c. Verify that there is internal consistency between the software requirements and external consistency with the system requirements. (2.3) Completeness a. Verify that the following elements are in the SRS or IRS, within the assumptions and constraints of the system: 1. Functionality (e.g., algorithms, state/mode definitions, input/output validation, exception handling, reporting, and logging); 2. Process definition and scheduling; 3. Hardware, software, and user interface descriptions. 4. Performance criteria (e.g., timing sizing, speed, capacity, accuracy, precision, safety, and security); 5. Critical configuration data; and 6. System, device, and software control (e.g., initialization, transaction and state monitoring, and self-testing). b. Verify that the SRS and IRS satisfy specified configuration management procedures. (2.4) Accuracy a. Validate that the logic, computational, and interface precision (e.g., truncation and rounding) satisfy the requirements in the system environment. b. Validate that the modeled physical phenomena conform to system accuracy requirements and physical laws. (2.5) Readability a. Verify that the documentation is legible, understandable, and unambiguous to the intended				

V&V Task	Required Outputs	GEH Process	GEH Outputs	Comments
audience. b. Verify that the documentation defines all acronyms, mnemonics, abbreviations, terms, and symbols. (2.6) Testability a. Verify that there are objective acceptance criteria for validating the requirements of the SRS and IRS.				
(3) Interface Analysis. Verify and validate that the requirements for software interfaces with hardware, user, operator, and other systems are correct, consistent, complete, accurate, and testable. The task criteria are as follows: (3.1) Correctness a. Validate the external and internal system and software interface requirements. (3.2) Consistency a. Verify that the interface descriptions are consistent between the SRS and IRS. (3.3) Completeness a. Verify that each interface is described and includes data format and performance criteria (e.g., timing, bandwidth, accuracy, safety, and security). (3.4) Accuracy a. Verify that each interface provides information with the required accuracy. (3.5) Testability a. Verify that there are objective acceptance criteria for validating the interface requirements.	Task Report(s) — Interface Analysis Anomaly Report(s)			
(4) Criticality Analysis. Review and update the existing criticality analysis results from the prior Criticality Task Report using the SRS and IRS. Implementation methods and interfacing technologies may cause previously assigned software integrity levels to be raised or lowered for a given software element (i.e., requirement, module, function, subsystem, other software partition). Verify that no inconsistent or undesired software integrity	Task Report(s) — Criticality Analysis Anomaly Report(s)			

V&V Task	Required Outputs	GEH Process	GEH Outputs	Comments
consequences are introduced by reviewing the revised software integrity levels.				
(5) System V&V Test Plan Generation and Verification. *(For Software Integrity Levels 3 and 4)* Plan system V&V testing to validate software requirements. Plan tracing of system requirements to test designs, cases, procedures, and results. Plan documentation of test designs, cases, procedures, and results. The System V&V Test Plan shall address the following: (1) compliance with all system requirements (e.g., functional, performance, security, operation, and maintenance) as complete software end items in the system environment; (2) adequacy of user documentation (e.g., training materials, procedural changes); and (3) performance at boundaries (e.g., data, interfaces) and under stress conditions. Verify that the System V&V Test Plan conform to Project defined test document purpose, format, and content (e.g., see IEEE Standard 8291983 [B5]). Validate that the System Test Plan satisfies the following criteria: (1) test coverage of system requirements; (2) appropriateness of test methods and standards used; (3) conformance to expected results; (4) feasibility of system qualification testing; and (5) feasibility and testability of operation and maintenance requirements.	Anomaly Report(s) System V&V Test Plan			
(6) Acceptance V&V Test Plan Generation and Verification. (For Software Integrity Levels 3 and 4) Plan Acceptance V&V testing to validate that software correctly implements system and software requirements in an operational environment. The task criteria are: (1) compliance with acceptance requirements in the operational environment, and (2) adequacy of user documentation. Plan tracing of acceptance test requirements to test design, cases, procedures, and execution results. Plan documentation of test tasks and results. Verify that the Acceptance V&V Test Plan complies with Project defined test document purpose, format, and content (e.g., see IEEE Standard 829-1983 [B5]). Validate that the Acceptance Test Plan satisfies	Acceptance V&V Test Plan Anomaly Report(s)			

V&V Task	Required Outputs	GEH Process	GEH Outputs	Comments
the following criteria: (1) test coverage of system requirements; (2) conformance to expected results; and (3) feasibility of operation and maintenance (e.g., capability to be operated and maintained in accordance with user needs).				
(7) Configuration Management Assessment. Verify that the Configuration Management process is complete and adequate. The task criteria are as follows: (7.1) Completeness a. Verify that there is a process for describing the software product functionality, tracking program versions, and managing changes. (7.2) Adequacy a. Verify that the configuration management process is adequate for the development complexity, software and system size, software integrity level, project plans, and user needs.	Task Report(s) — Configuration Management Assessment Anomaly Report(s)			
(8) Hazard Analysis. Determine software contributions to system hazards. The hazard analysis shall: (1) identify the software requirements that contribute to each system hazard; and (2) validate that the software addresses, controls, or mitigates each hazard.	Task Report(s) — Hazard Analysis Anomaly Report(s)			
(9) Risk Analysis. Review and update risk analysis using prior task reports. Provide recommendations to eliminate, reduce, or mitigate the risks.	Task Report(s) — Risk Analysis Anomaly Report(s)			]]

V&V Task	Required Outputs	GEH Process	GEH Outputs	Comments
5.4.3 Design V&V activity (developing process)				
	Task Report(s) — Traceability Analysis Anomaly Report(s)	[[		
(2) Software Design Evaluation. Evaluate the design elements (SDD and IDD) for correctness, consistency, completeness, accuracy, readability, and testability. The task criteria are as follows: (2.1) Correctness a. Verify and validate that the source code component satisfies the software design. b. Verify that the source code components comply with standards, references, regulations, policies, physical laws, and business rules. c. Validate the source code component sequences of states and state changes using logic and data flows coupled with domain expertise, prototyping results, engineering principles, or other basis. d. Validate that the flow of data and control satisfy functionality and performance requirements. e. Validate data usage and format. f. Assess the appropriateness of coding methods and standards. (2.2) Consistency a. Verify that all terms and code concepts are documented consistently. b. Verify that there is internal consistency between the source code components. (2.3) Completeness	Task Report(s) — Software Design Evaluation Anomaly Report(s)			

V&V Task	Required Outputs	GEH Process	GEH Outputs	Comments
a. Verify that the following elements are in the SDD, within the assumptions and constraints of the system: 1. Functionality (e.g., algorithms, state/mode definitions, input/output validation, exception handling, reporting and logging); 2. Process definition and scheduling; 3. Hardware, software, and user interface descriptions; 4. Performance criteria (e.g., timing, sizing, speed, capacity, accuracy, precision, safety, and security); 5. Critical configuration data; 6. System, device, and software control (e.g., initialization, transaction and state monitoring, and self-testing). b. Verify that the SDD and IDD satisfy specified configuration management procedures. (2.4) Accuracy a. Validate that the logic, computational, and interface precision (e.g., truncation and rounding) satisfy the requirements in the system environment. b. Validate that the modeled physical phenomena conform to system accuracy requirements and physical laws. (2.5) Readability a. Verify that the documentation is legible, understandable, and unambiguous to the intended audience. b. Verify that the documentation defines all acronyms, mnemonics, abbreviations, terms, symbols, and design language, if any. (2.6) Testability a. Verify that there are objective acceptance criteria for validating each software design element and the				

V&V Task	Required Outputs	GEH Process	GEH Outputs	Comments
system design. b. Verify that each software design element is testable to objective acceptance criteria.				
(3) Interface Analysis. Verify and validate that the software design interfaces with hardware, user, operator, software, and other systems for correctness, consistency, completeness, accuracy, and testability. The task criteria are as follows: (3.1) Correctness a. Validate the external and internal software interface design in the context of system requirements. (3.2) Consistency a. Verify that the interface design is consistent between the SDD and IDD. (3.3) Completeness a. Verify that each interface is described and includes data format and performance criteria (e.g., timing, bandwidth, accuracy, safety, and security). (3.4) Accuracy a. Verify that each interface provides information with the required accuracy. (3.5) Testability a. Verify that there are objective acceptance criteria for validating the interface design.	Task Report(s) — Interface Analysis Anomaly Report(s)			
(4) Criticality Analysis. Review and update the existing criticality analysis results from the prior Criticality Task Report using the SDD and IDD. Implementation methods and interfacing technologies may cause previously assigned software integrity levels to be raised or lowered for a given software element (i.e., requirement, module, function, subsystem, other software partition). Verify that no inconsistent or undesired software integrity consequences are introduced by reviewing the revised software integrity levels.	Task Report(s) — Criticality Analysis Anomaly Report(s)			

V&V Task	Required Outputs	GEH Process	GEH Outputs	Comments
(5) Component V&V Test Plan Generation and Verification. *(For Software Integrity Levels 3 and 4.)* Plan component V&V testing to validate that the software components (e.g., units, source code modules) correctly implement component requirements. The task criteria are: (1) compliance with design requirements; (2) assessment of timing, sizing, and accuracy; (3) performance at boundaries and interfaces and under stress and error conditions; and (4) measures of requirements test coverage and software reliability and maintainability. Plan tracing of design requirements to test design, cases, procedures, and results. Plan documentation of test tasks and results. Verify that the Component V&V Test Plan complies with Project defined test document purpose, format, and content (e.g., see IEEE Standard 829-1983 [B5]). Validate that the Component V&V Test Plan satisfies the following criteria: (1) traceable to the software requirements and design; (2) external consistency with the software requirements and design; (3) internal consistency between unit requirements; (4) test coverage of requirements in each unit; (5) feasibility of software integration and testing; and (6) feasibility of operation and maintenance (e.g., capability to be operated and maintained in accordance with user needs).	Component V&V Test Plan Anomaly Report(s)			
(6) Integration V&V Test Plan Generation and Verification. (For Software Integrity Levels 3 and 4.) Plan integration testing to validate that the software correctly implements the software requirements and design as each software component (e.g., units or modules) is incrementally integrated with each other. The task criteria are: (1) compliance with increasingly larger set of functional requirements at each stage of integration; (2) assessment of timing, sizing, and accuracy; (3) performance at boundaries and under stress conditions; and (4) measures of requirements test coverage and software reliability. Plan tracing of requirements to test design, cases, procedures, and results. Plan documentation of test tasks and results. Verify that the Integration V&V Test Plan complies with Project defined test document purpose, format, and content (e.g., see IEEE Standard 829-1983 [B5]). Validate that the Integration V&V Test Plan satisfies the	Integration V&V Test Plan Anomaly Report(s)			

V&V Task	Required Outputs	GEH Process	GEH Outputs	Comments
following criteria: (1) traceable to the system requirements; (2) external consistency with the system requirements; (3) internal consistency; (4) test coverage of the software requirements; (5) appropriateness of test standards and methods used; (6) conformance to expected results; (7) feasibility of software qualification testing; and (8) feasibility of operation and maintenance (e.g., capability to be operated and maintained in accordance with user needs).				
(7) V&V Test Design Generation and Verification. (For Software Integrity Levels 3 and 4.) Design tests for: (1) component testing; (2) integration testing; (3) system testing; and (4) acceptance testing. Continue tracing required by the V&V Test Plan. Verify that the V&V Test Designs comply with Project defined test document purpose, format, and content (e.g., see IEEE Standard 829-1983 [B5]). Validate that the V&V Test Designs satisfy the criteria in V&V tasks 5.4.3 Task 5; 5.4.3 Task 6; 5.4.2 Task 5; and 5.4.2 Task 6, for component, integration, system, and acceptance testing, respectively.	Component V&V Test Design(s) Integration V&V Test Design(s) System V&V Test Design(s) Acceptance V&V Test Design(s) Anomaly Report(s)			
8) Hazard Analysis. Verify that logic design and associated data elements correctly implement the critical requirements and introduce no new hazards. Update the hazard analysis.	Task Report(s) — Hazard Analysis Anomaly Report(s)			
(9) Risk Analysis. Review and update risk analysis using prior task reports. Provide recommendations to eliminate, reduce, or mitigate the risks.	Task Report(s) — Risk Analysis Anomaly Report(s)			]]

V&V Task	Required Outputs	GEH Process	GEH Outputs	Comments
5.4.4 Implementation V&V Activity (development process)				
(1) Traceability Analysis. Trace the source code components to corresponding design specification(s), and design specification(s) to source code components. Analyze identified relationships for correctness, consistency, and completeness. The task criteria are as follows: (1.1) Correctness a. Validate the relationship between the source code components and design element(s). (1.2) Consistency a. Verify that the relationships between the source code components and design elements are specified to a consistent level of detail. (1.3) Completeness a. Verify that all source code components are traceable from the design elements. b. Verify that all design elements are traceable to the source code components.	Task Report(s) — Traceability Analysis Anomaly Report(s)	[[		
(2) Source Code and Source Code Documentation Evaluation. Evaluate the source code components (Source Code Documentation) for correctness, consistency, completeness, accuracy, readability, and testability. The task criteria are as follows: (2.1) Correctness a. Verify and validate that the source code component satisfies the software design. b. Verify that the source code components comply with standards, references, regulations, policies, physical laws, and business rules. c. Validate the source code component sequences of states and state changes using logic and data flows coupled with domain expertise, prototyping results, engineering principles, or other basis. d. Validate that the flow of data and control satisfy	Task Report(s) — Source Code and Source Code Documentation Evaluation Anomaly Report(s)			

V&V Task	Required Outputs	GEH Process	GEH Outputs	Comments
functionality and performance requirements. e. Validate data usage and format. f. Assess the appropriateness of coding methods and standards. (2.2) Consistency a. Verify that all terms and code concepts are documented consistently. b. Verify that there is internal consistency between the source code components. c. Validate external consistency with the software design and requirements. (2.3) Completeness a. Verify that the following elements are in the source code, within the assumptions and constraints of the system: 1. Functionality (e.g., algorithms, state/mode definitions, input/output validation, exception handling, reporting and logging); 2. Process definition and scheduling; 3. Hardware, software, and user interface descriptions; 4. Performance criteria (e.g., timing, sizing, speed, capacity, accuracy, precision, safety, and security); 5. Critical configuration data; 6. System, device, and software control (e.g., initialization, transaction and state monitoring, and self-testing). b. Verify that the source code documentation satisfies specified configuration management procedures. (2.4) Accuracy a. Validate the logic, computational, and interface precision (e.g., truncation and rounding) in the system environment. b. Validate that the modeled				

V&V Task	Required Outputs	GEH Process	GEH Outputs	Comments
physical phenomena conform to system accuracy requirements and physical laws. (2.5) Readability a. Verify that the documentation is legible, understandable, and unambiguous to the intended audience. b. Verify that the documentation defines all acronyms, mnemonics, abbreviations, terms, and symbols. (2.6) Testability a. Verify that there are objective acceptance criteria for validating each source code component. b. Verify that each source code component is testable against objective acceptance criteria.				
(3) Interface Analysis. Verify and validate that the software source code interfaces with hardware, user, operator, software, and other systems for correctness, consistency, completeness, accuracy, and testability. The task criteria are as follows: (3.1) Correctness a. Validate the external and internal software interface code in the context of system requirements. (3.2) Consistency a. Verify that the interface code is consistent between source code components and to external interfaces (i.e., hardware, user, operator, and other software). (3.3) Completeness a. Verify that each interface is described and includes data format and performance criteria (e.g., timing, bandwidth, accuracy, safety, and security). (3.4) Accuracy a. Verify that each interface provides information with the required accuracy. (3.5) Testability a. Verify that there are objective acceptance criteria	Task Report(s) — Interface Analysis Anomaly Report(s)			

V&V Task	Required Outputs	GEH Process	GEH Outputs	Comments
for validating the interface code.				
(4) Criticality Analysis. Review and update the existing criticality analysis results from the prior Criticality Task Report using the source code. Implementation methods and interfacing technologies may cause previously assigned software integrity levels to be raised or lowered for a given software element (i.e., requirement, module, function, subsystem, other software partition). Verify that no inconsistent or undesired software integrity consequences are introduced by reviewing the revised software integrity levels.	Task Report(s) — Criticality Analysis Anomaly Report(s)			
(5) V&V Test Case Generation and Verification. (For Software Integrity Levels 3 and 4.) Develop V&V Test Cases for: (1) component testing; (2) integration testing; (3) system testing; and (4) acceptance testing. Continue tracing required by the V&V Test Plans. Verify that the V&V Test Cases comply with Project defined test document purpose, format, and content (e.g., see IEEE Standard 829-1983 [B5]). Validate that the V&V Test Cases satisfy the criteria in V&V tasks 5.4.3 Task 5; 5.4.3 Task 6; 5.4.2 Task 5; and 5.4.2 Task 6 for component, integration, system, and acceptance testing, respectively.	Component V&V Test Cases Integration V&V Test Cases System V&V Test Cases Acceptance V&V Test Cases Anomaly Report(s)			

V&V Task	Required Outputs	GEH Process	GEH Outputs	Comments
(6) V&V Test Procedure Generation and Verification. (For Software Integrity Levels 3 and 4.) Develop V&V Test Procedures for: (1) component testing; (2) integration testing; and (3) system testing. Continue tracing required by the V&V Test Plans. Verify that the V&V Test Procedures comply with Project defined test document purpose, format, and content (e.g., see IEEE Standard 829-1983 [B5]). Validate that the V&V Test Procedures satisfy the criteria in V&V tasks 5.4.3 Task 5; 5.4.3 Task 6; and 5.4.2 Task 5 for component, integration, and system testing, respectively.	Component V&V Test Procedures Integration V&V Test Procedures System V&V Test Procedures Anomaly Report(s)			
7) Component V&V Test Execution and Verification. (For Software Integrity Levels 3 and 4.) Perform V&V component testing. Analyze test results to validate that software correctly implements the design. Validate that the test results trace to test criteria established by the test traceability in the test planning documents. Document the results as required by the Component V&V Test Plan. Use the V&V component test results to validate that the software satisfies the V&V test acceptance criteria. Document discrepancies between actual and expected test results.	Task Report(s) — Test Results Anomaly Report(s)			
(8) Hazard Analysis. Verify that the implementation and associated data elements correctly implement the critical requirements and introduce no new hazards. Update the hazard analysis.	Task Report(s) — Hazard Analysis Anomaly Report(s)			
(9) Risk Analysis. Review and update risk analysis using prior task reports. Provide recommendations to eliminate, reduce, or mitigate the risks.	Task Report(s) — Risk Analysis Anomaly Report(s)			]]
5.4.5 Test V&V Activity (development process)				
(1) Traceability Analysis. Analyze relationships in the V&V Test Plans, Designs, Cases, and Procedures for correctness and completeness. For correctness, verify that there is a valid relationship between the V&V Test Plans, Designs, Cases, and Procedures. For completeness, verify that all V&V Test Procedures are traceable to the V&V Test Plans.	Task Report(s) — Traceability Analysis Anomaly Report(s)	[[		

V&V Task	Required Outputs	GEH Process	GEH Outputs	Comments
(2) Acceptance V&V Test Procedure Generation and Verification. (For Software Integrity Levels 3 and 4.) Develop Acceptance V&V Test Procedures. Continue the tracing required by the Acceptance V&V Test Plan. Verify that the V&V Test Procedures comply with Project defined test document purpose, format, and content (e.g., see IEEE Standard 829-1983 [B5]). Validate that the Acceptance V&V Test Procedures satisfy the criteria in V&V task 5.4.2 Task 6.	Acceptance V&V Test Procedure Anomaly Report(s)			
(3) Integration V&V Test Execution and Verification. (For Software Integrity Levels 3 and 4.) Perform V&V integration testing. Analyze test results to verify that the software components are integrated correctly. Validate that the test results trace to test criteria established by the test traceability in the test planning documents. Document the results as required by the Integration V&V Test Plan. Use the V&V integration test results to validate that the software satisfies the V&V test acceptance criteria. Document discrepancies between actual and expected test results.	Task Report(s) — Test Results Anomaly Report(s)			
(4) System V&V Test Execution and Verification. *(For Software Integrity Levels 3 and 4.)* Perform V&V system testing. Analyze test results to validate that the software satisfies the system requirements. Validate that the test results trace to test criteria established by the test traceability in the test planning documents. Document the results as required by the System V&V Test Plan. Use the V&V system test results to validate that the software satisfies the V&V test acceptance criteria. Document discrepancies between actual and expected test results.	Task Report(s) — Test Results Anomaly Report(s)			

V&V Task	Required Outputs	GEH Process	GEH Outputs	Comments
(5) Acceptance V&V Test Execution and Verification. *(For Software Integrity Levels 3 and 4.)* Perform acceptance V&V testing. Analyze test results to validate that the software satisfies the system requirements. Validate that the test results trace to test criteria established by the test traceability in the test planning documents. Document the results as required by the Acceptance V&V Test Plan. Use the acceptance V&V test results to validate that the software satisfies the V&V test acceptance criteria. Document discrepancies between actual and expected test results.	Task Report(s) — Test Results Anomaly Report(s)			
(6) Hazard Analysis. Verify that the test instrumentation does not introduce new hazards. Update the hazard analysis.	Task Report(s) — Hazard Analysis Anomaly Report(s)			
(7) Risk Analysis. Review and update risk analysis using prior task reports. Provide recommendations to eliminate, reduce, or mitigate the risks.	Task Report(s) — Risk Analysis Anomaly Report(s)			]]
5.4.6 Installation and Checkout V&V Activity (development process)				
(1) Installation Configuration Audit. Verify that all software products required to correctly install and operate the software are present in the installation package. Validate that all site dependent parameters or conditions to verify supplied values are correct.	Task Report(s) — Installation Configuration Audit Anomaly Report(s)	[[		
(2) Installation Checkout. Conduct analyses or tests to verify that the installed software corresponds to the software subjected to V&V. Verify that the software code and databases initialize, execute, and terminate as specified. In the transition from one version of software to the next, the V&V effort shall validate that the software can be removed from the system without affecting the functionality of the remaining system components. The V&V effort shall verify the requirements for continuous operation and service during transition, including user notification.	Task Report(s) — Installation Checkout Anomaly Report(s)			[[ ]]
(3) Hazard Analysis. Verify that the installation procedures and installation environment does not introduce new hazards. Update the hazard analysis.	Task Report(s) — Hazard Analysis Anomaly Report(s)			

V&V Task	Required Outputs	GEH Process	GEH Outputs	Comments
(4) Risk Analysis. Review and update risk analysis using prior task reports. Provide recommendations to eliminate, reduce, or mitigate the risks.	Task Report(s) — Risk Analysis Anomaly Report(s)			
(5) V&V Final Report Generation. Summarize in the V&V final report the V&V activities, tasks and results, including status and disposition of anomalies. Provide an assessment of the overall software quality and provide recommendations.	V&V Final Report		]]	
5.5.1 Operation V&V Activity (operation process)				
(1) Evaluation of New Constraints. Evaluate new constraints (e.g., operational requirements, platform characteristics, operating environment) on the system or software requirements to verify the applicability of the SVVP. Software changes are maintenance activities (see 5.6.1).	Task Report(s) — Evaluation of New Constraints	[[		[[
(2) Proposed Change Assessment. Assess proposed changes (e.g., modifications, enhancements, or additions) to determine the effect of the changes on the system. Determine the extent to which V&V tasks would be iterated.	Task Report(s) — Proposed Change Assessment			]]
(3) Operating Procedures Evaluation. Verify that the operating procedures are consistent with the user documentation and conform to the system **requirements.**	Task Report(s) — Operating Procedures Evaluation Anomaly Report(s)			
(4) Hazard Analysis. Verify that the operating procedures and operational environment does not introduce new hazards. Update the hazard analysis.	Task Report(s) — Hazard Analysis Anomaly Report(s)			
(5) Risk Analysis. Review and update risk analysis using prior task reports. Provide recommendations to eliminate, reduce, or mitigate the risks.	Task Report(s) — Risk Analysis Anomaly Report(s)		]]	

V&V Task	Required Outputs	GEH Process	GEH Outputs	Comments
5.6.1 Maintenance V&V Activity (maintenance process)				
(1) SVVP Revision. Revise the SVVP to comply with approved changes. When the development documentation required by this standard is not available, generate a new SVVP and consider the methods in Annex D (V&V of reusable software) for deriving the required development documentation.	Updated SVVP	[[		[[
(2) Proposed Change Assessment. Assess proposed changes (i.e., modifications, enhancements, or additions) to determine the effect of the changes on the system. Determine the extent to which V&V tasks would be iterated.	Task Report(s) — Proposed Change Assessment			
(3) Anomaly Evaluation. Evaluate the effect of software operation anomalies.	Task Report(s) — Anomaly Evaluation			
(4) Criticality Analysis. Determine the software integrity levels for proposed modifications. Validate the integrity levels provided by the maintainer. For V&V planning purposes, the highest software integrity level assigned to the software shall be the software system integrity level.	Task Report(s) — Criticality Analysis Anomaly Report(s)			]]
(5) Migration Assessment. Assess whether the software requirements and implementation address 1) specific migration requirements, 2) migration tools, 3) conversion of software products and data, 4) software archiving, 5) support for the prior environment, and 6) user notification.	Task Report(s) — Migration Assessment Anomaly Report(s)			
(6) Retirement Assessment. For software retirement, assess whether the installation package addresses: 1) software support, 2) effect on existing systems and databases, 3) software archiving, 4) transition to a new software product, and 5) user notification.	Task Report(s) — Retirement Assessment Anomaly Report(s)			
(7) Hazard Analysis. Verify that software modifications correctly implement the critical requirements and introduce no new hazards. Update the hazard analysis.	Task Report(s) — Hazard Analysis Anomaly Report(s)			
(8) Risk Analysis. Review and update risk analysis using prior task reports. Provide recommendations to eliminate, reduce, or mitigate the risks.	Task Report(s) — Risk Analysis Anomaly Report(s)			

V&V Task	Required Outputs	GEH Process	GEH Outputs	Comments
(9) Task Iteration. Perform V&V tasks, as needed, to ensure that 1) planned changes are implemented correctly; 2) documentation is complete and current; and 3) changes do not cause unacceptable or unintended system behaviors.	Task Report(s) Anomaly Report(s)		]]	

Table 4.4-7 Mapping of RG 1.169 Position 7

RG 1.168 Paragraph	Description	GEH Program/Approach	GEH Process	Comment
C. REGULATORY POSITION - 7. Verification and Validation Tasks	Table 3 of IEEE Standard 1012-1998 lists "optional" V&V tasks. These are further described in Annex G (which is for information only) to IEEE Standard 1012-1998. These tasks are intended to provide a tailoring capability by allowing tasks to be added to the minimum set for critical software. Exception is taken to the "optional" status of some tasks on this list; they are considered by the NRC staff to be necessary components of acceptable methods for meeting the requirements of Appendices A and B to 10 CFR Part 50 as applied to software, regardless of whether they are performed by the V&V organization. The following tasks are considered by the NRC staff to be part of the minimum set of V&V activities for critical software unless they are (1) incorporated into other V&V tasks in the SVVP or (2) performed outside the software V&V organization as part or all of the duties of some other organization.	[[		
C. REGULATORY POSITION - 7. Verification and Validation Tasks. 7.1 Audits	Criterion I of Appendix B defines quality assurance functions as including verifying, such as by checking, auditing, and inspection, that activities affecting safety-related functions have been correctly performed. Criterion III requires design control measures for verifying or checking the adequacy of design. Safety system software V&V organizations may employ			

RG 1.168 Paragraph	Description	GEH Program/Approach	GEH Process	Comment
	audits, including functional audits, in-process audits, and physical audits of software. Although these audits are commonly considered to be the responsibility of the software quality assurance organization and the configuration management organization, they may be performed and relied upon by the V&V organization. If so, the audits should be described in the SVVP. An acceptable method of conducting these audits is described in IEEE Standard 1028-1997.			
C. REGULATORY POSITION - 7. Verification and Validation Tasks. 7.2 Regression Analysis and Testing	Criterion III, "Design Control," requires that design changes be subject to design control measures commensurate with those applied to the original design. Regression analysis and testing following the implementation of software modifications is an element of the V&V of software changes. It is considered by the NRC staff to be part of the minimum set of software V&V activities for safety system software.			
C. REGULATORY POSITION - 7. Verification and Validation Tasks. 7.3 Security Assessment	A security breach of a digital system containing safety system software has the potential to prevent that software from fulfilling its safety function. Appendix A imposes functional and reliability requirements with respect to safety systems. According to 10 CFR 73.46, vital equipment (which includes safety system			

RG 1.168 Paragraph	Description	GEH Program/Approach	GEH Process	Comment
	software) must be protected by physical barriers and access control. The NRC staff considers security assessment of safety system software to be part of the minimum set of software V&V activities for such software.			
C. REGULATORY POSITION - 7. Verification and Validation Tasks. 7.4 Test Evaluation	Test evaluation includes confirming the technical adequacy of test materials such as plans, designs, and results. These materials are evaluated for consistency with Criterion II, "Quality Assurance Program," in its requirement for controlled conditions, and with Criterion XI, "Test Control," in its requirement for the evaluation of test results.			

RG 1.168 Paragraph	Description	GEH Program/Approach	GEH Process	Comment
C. REGULATORY POSITION - 7. Verification and Validation Tasks. 7.5 Evaluation of User Documentation	User documentation is important to the safe operation and proper maintenance of safety system software. The requirements of Criterion III, "Design Control," for correctly translating the design basis of safety system software into specifications, procedures, drawings, and instructions, apply to software documentation, including user documentation.			]]

5. Environmental Equipment Qualification

The Equipment Qualification testing includes exposure to temperature, humidity, radiation, electromagnetic and radio interference, and seismic input. This information is found in the equipment qualifications test plans, methodologies, and test reports. The results of the PRNM instrument qualification testing are provided in Section 5.4.1-5.4.5 (Environmental), Section 5.4.6 (Seismic), and Section 5.4.7 (Electromagnetic Compatibility (EMC)). The NIC instrument qualification is provided in Section 5.4.8. The effect of a single failure within the Environmental Control (Control Room Ventilation) System is provided in Section 5.4.9.

The information provided supports the conclusion that the worst case CGS main control room environment in which the CGS PRNMS needs to operate will not have a negative effect on the ability of the CGS PRNMS to perform its safety function. The equipment qualification provides a comparison that shows that the equipment qualifications envelopes the worst case CGS MCR environmental conditions for each environmental stressor.

5.1 Equipment Covered

The conclusions and equipment capability, documented in GEH PRNM Qualification Summary for CGS (Reference 72), apply to CGS for the specific equipment items identified in Table 5-1. The NIC instrument qualification is provided in Section 5.4.8.

Table 5-1 Equipment Covered

[[
]]

5.2 Equipment Qualification

In accordance with the Reference 1, both the documentation of the qualification activities and the required confirmation "should be included in the plant-specific licensing submittal." This section provides the analyses and reference documents that demonstrate the environmental conditions for the CGS PRNM System configuration are enveloped by the conditions to which GEH NUMAC PRNM System equipment has been qualified as discussed in Section 4.4.2 of Reference 1 and as required in Section 5.0, item 4 of the original SER for the LTR.

The main control room at CGS is considered a mild environment for all design basis events (DBEs) and accidents. The License Basis for CGS does not require qualification of safety-related equipment in the main control room. New PRNM equipment being installed in the main control room must meet the environmental design conditions for the main control room. The CGS specific analyses and testing performed to support qualification of the CGS PRNM equipment as installed in CGS is documented (Reference 73).

[[

]] An instrument-by-instrument comparison of the CGS PRNM instruments to the generic PRNM instruments is provided in the CGS PRNM Qualification Summary (Reference 72).

5.3 Regulatory Evaluation

Regulatory criteria for environmental qualifications of safety-related equipment are provided in:

Harsh Environment: 10 CFR 50.49, "Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants,"

10 CFR Part 50, Appendix A:

GDC 2, "Design Bases for protection Against Natural Phenomena," and

GDC 4, "Environmental and Dynamic Effects Design Bases."

10 CFR 50.55a(h) incorporates (based on the date of that the construction permit was issued):

IEEE Standard 279-1971 (see Clause 4.4, "Equipment Qualification"), and

IEEE Standard 603-1991 (see Clause 5.4, "Equipment Qualification").

RG 1.152 Revision 2, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," endorses IEEE Standard 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations"; Clause 5.4, "Equipment Qualification" contains guidance on equipment qualification.

RG 1.180 Revision 1, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," endorses several standards.

Harsh Environment: RG 1.89 Revision 1, "Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plant," endorses IEEE Standard 323-1974, "IEEE Standard for Qualifying Class IE Equipment for Nuclear Power Generating Stations," subject to the regulatory positions described in the RG, and as supplemented by RG 1.209.

Mild Environment: RG 1.209 dated March 2007, "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants," endorses IEEE Standard 323-2003 subject to five enhancements and exceptions.

SRP (NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition") Chapter 7, "Instrumentation and Controls," Appendix 7.0-A "Review Process for Digital Instrumentation and Control Systems" Section B.1, "Qualification of Digital Instrumentation and Control Systems and Components," contains guidance on equipment qualification.

Appendix 7.1-B "Guidance for Evaluation of Conformance to IEEE Standard 279" Section 4.4, "Equipment Qualification," contains guidance on equipment qualification.

Appendix 7.1-C "Guidance for Evaluation of Conformance to IEEE Standard 603" Section 5.4, "Equipment Qualification," contains guidance on equipment qualification.

Appendix 7.1-D "Guidance for Evaluation of Conformance to IEEE Standard 7-4.3.2" Section 5.4, "Equipment Qualification," contains guidance on equipment qualification.

Regulatory Guide 1.209 endorses guidance for compliance with IEEE Standard 323-2003. Mild environment qualification should conform with the guidance of IEEE Standard 323-2003. The information provided should demonstrate how the equipment was tested, or what analysis was done. The resultant test data or analysis should also be provided to allow the NRC staff to make a determination that the testing or analysis was adequate and demonstrate that the environmental qualification envelopes the worst case accident conditions in the location where the equipment should be located for any event where the equipment is credited for mitigation.

Additionally, the licensee should show why a single failure within the environmental control system, for any area in which safety system equipment is located, should not result in conditions that could result in damage to the safety system equipment, nor prevent the balance of the safety system not within the area from accomplishing its safety function. In this regard, the loss of a safety-related environmental control system is treated as a single failure that should not prevent the safety system from accomplishing its safety functions. Non safety-related environmental control systems should be postulated to fail.

Because the loss of environmental control systems does not usually result in prompt changes in environmental conditions, the design bases may rely upon monitoring environmental conditions and taking appropriate action to ensure that extremes in environmental conditions are maintained within non-damage limits until the environmental control systems are returned to normal

operation. If such bases are used, the licensee should demonstrate that there is independence between environmental control systems and sensing systems that would indicate the failure or malfunctioning of environmental control systems.

Regulatory Guide 1.151 dated July 1983, "Instrument Sensing Lines," may be used to ensure that the environmental protection of instrument sensing lines is addressed.

Electro Magnetic Interference (EMI) qualification in accordance with the guidance of Regulatory Guide 1.180, Revision 1, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," is an acceptable means of meeting the qualification requirements for EMI and electrostatic discharge (ESD).

Lightning protection should be addressed as part of the review of electromagnetic compatibility.

Regulatory Guide 1.204, "Guidelines for Lightning Protection of Nuclear Power Plants," provides additional guidance.

Additional disciplines should be involved in the review of equipment qualification to harsh environments, seismic events, evaluation of conformance to the requirements of GDC 2 and 4 and 10 CFR 50.49 to ensure the requirements for equipment qualification to harsh environments and seismic events are met. Guidance for the review of this equipment qualification is given in SRP Sections 3.10 and 3.11.

SRP Appendix 7.1-D subsection 5.4 provides additional guidance on environmental qualification of digital computers for use in safety systems.

5.4 CGS PRNM Panel Environmental Requirements

Table 5-2 provides the Reference 1 levels to which the PRNM is qualified. Table 5-3 provides the CGS PRNM Panel Environmental Requirements within the CGS main control room. A comparison to the CGS PRNM Panel Environmental Requirements and justification of CGS PRNM equipment qualification follows.

Table 5-2 PRNM Instrument Environmental Qualifications

Parameter	Minimum	Nominal	Maximum	U/M
Temperature, Operating	[[			
Humidity, Operating				
Pressure, Static				
Radiation, Gamma Rate				
Radiation, Gamma TID				
Qualified Life				]]

TID: Total Integrated Dose

Table 5-3 CGS PRNM Panel Environmental Requirements (1)

Parameter	Minimum	Nominal	Maximum	U/M
Temperature	[[			
Humidity, Operating				
Pressure				
Radiation, Gamma Rate				
Radiation, Gamma TID				]]

(1) Values from NUMAC PRNM System Requirements Data Sheet, CGS (Reference 5)
NS = Not Specified

5.4.1 Temperature

To demonstrate qualification of the PRNMS instruments at the installed locations, it is necessary to determine the temperature rise in the mounting cabinet. [[

]] For testing, the margin in IEEE 323-1974 (Reference 74) of 15°F was added to the required test temperature (139°F). All PRNM equipment has been tested to 142°F giving an additional 3°F margin. The tested capability exceeds the maximum allowed control room conditions including internal heat rise.

The minimum design limit for the main control room is 40°F. [[

]] As addressed in the GEH Qualification Documentation, all PRNM equipment has been tested to 4.44°C (40°F). The minimum main control room temperature is 40°F, equal to the minimum qualified temperature of 40°F (4.44°C). Therefore, the new PRNM equipment is capable of functioning in the lowest design basis ambient temperature for the main control room.

5.4.1.1 Other Margin

To support coping with a station blackout event, the main control room is required to operate at 75°F + or – 3°F (72°F to 78°F). This operating envelope is controlled by the LCS.

5.4.2 Humidity

The design basis humidity conditions for the MCR are 10% to 60% RH. The PRNM equipment is designed for ambient humidity of 20% to 90% RH (non-condensing). The equipment was tested in humidity conditions of 20% to 90% RH. The MCR upper design basis value of 60% RH is bounded by the testing performed. The test equipment was limited to a lower humidity level of 20% RH. The CGS requirements include operation down to 10% RH compared to the minimum qualified level of 20% RH. GEH has analyzed the PRNM equipment and determined low humidity was not a concern. The low humidity can challenge some equipment by drying out components or producing conditions that promote ESDs. However, based on a review by GEH, the PRNM equipment does not contain components susceptible to drying out. ESD testing was

successfully conducted on the equipment as part of the EMC qualification. In addition, the CGS plant includes operating procedures to reduce or eliminate the risk of ESD damage to equipment. Therefore, the PRNM components are qualified to relative humidity levels down to 10% RH without adverse effects on system performance. Recently performed environmental testing of NUMAC equipment similar to the CGS PRNM components using improved environmental chambers further supports this conclusion. A study of actual humidity conditions at the site over a two year time period showed that the lowest daily average humidity was 19% rh. Based on the Heating, Ventilating, and Air Conditioning (HVAC) design for the control room the ambient humidity is representative of the outside average humidity rather than the lowest level during the day.

Based on testing and analysis, the PRNM equipment has been shown to be capable of functioning in the humidity range inside the MCR during normal and DBE/accident conditions.

5.4.3 Pressure

The CGS normal ambient atmospheric pressure is approximately 14.43 psia (nominally 14.0-15.0 psia). The MCR ambient pressure conditions are the same as normal atmospheric conditions except during a DBE loss-of-coolant accident (LOCA) when the MCR is pressurized to around 1" WC to maintain habitability. The PRNM equipment was tested from 13-16 psi which envelops the required conditions.

5.4.4 Radiation

The MCR uses shielding and HVAC pressurization during accident conditions to limit radiation exposure to operating personnel. The normal operating design limit for the MCR is < 1 mR/hr and a TID gamma dose over 40 years of 350 Rad. During accident conditions the main control room dose is limited to less than 5 Rads in 30 days. The PRNM equipment was tested at 0.5 mR/hr up to 1000 Rads TID gamma. The testing exceeds the required dose.

5.4.5 Sprays and Chemicals

The PRNM equipment will not be exposed to sprays (e.g. fire sprinkler system) and chemicals. The fire suppression system located in the MCR is Halon (gas) and there is no chemical storage allowed in this area.

5.4.6 Seismic Qualification

Because the PRNM equipment is safety-related, it has been seismically qualified by GEH to the requirements of IEEE Standard 344-1975 (Reference 75). Analysis was used to determine the seismic accelerations at the PRNM equipment mounting locations and testing was used to qualify the equipment for the required seismic accelerations.

5.4.6.1 Seismic Qualification Overview

The CGS Seismic Qualification Report (Reference 73) presents the technical basis for qualification of the PRNM equipment and hardware that will be installed in the existing equipment control panel P608 of the CGS main control room. The following purpose and conclusions are based on the seismic analysis completed for the CGS PRNM enclosure that is

being modified to accommodate the upgrade to the NUMAC PRNM equipment.

5.4.6.2 Seismic Qualification (Operability) of the NUMAC Equipment

[[

]]

5.4.6.3 Seismic Qualification (Operability) of the Non-NUMAC Safety Related Equipment

There is no safety related equipment in the original panel assembly that remains in the modified assembly.

5.4.6.4 Seismic Qualification of Control Room Panel P603

The control room is located in a Safety Class 3, Seismic Category I structure. Safe occupancy of the control room during abnormal conditions is ensured by the design. Adequate shielding is provided to maintain tolerable radiation levels in the control room in the event of a design basis accident for the duration of the accident.

The initial seismic qualification of GE-supplied electrical equipment was based on single frequency "continuous" testing in which the applied vibration was a sinusoidal table motion at a fixed peak acceleration and a discrete frequency at any given time. Each frequency and acceleration combination was maintained for about 30 sec except when a resonance search was made (see Reference 75). The vibratory excitation was applied in three orthogonal axes individually with the axes chosen as those coincident with the most probable mounting configuration.

The first step was to search for resonances in each device. This was done because resonances cause amplification of the input vibration and are the most likely cause of malfunction or spurious operation. The resonance search was usually run at low acceleration levels (0.2g) to avoid destroying the test sample in case a severe resonance was encountered. The search was made from 0.25 Hz to 33 Hz in accordance with Reference 75 for a test period of no less than 7 minutes; if the device was large enough, the vibrations were monitored by accelerometers placed at critical locations from which resonances were determined by comparing the

acceleration level with that at the table of the vibration machine. Usually, the devices were either too small for an accelerometer, had their critical parts in an inaccessible location, or had critical parts that would be adversely affected by the mounting of an accelerometer. In these cases, the resonances were detected visually (strobe light), by audible observation, or by performance.

Following the frequency scan and resonance determination, the devices were tested to determine their malfunction limit. The malfunction limit test was run at each resonant frequency as determined by the frequency scan. In this test, the acceleration level was gradually increased until either the device malfunctioned or the limit of the vibration machine was reached. If no resonances were detected (as was usually the case), the device was considered to be rigid (all parts move in unison) and the malfunction limit was therefore independent of frequency. To achieve maximum acceleration from the vibration machine, rigid devices were malfunction tested at the upper test frequency (33 Hz,) because that allowed the maximum acceleration to be obtained from deflection-limited machines.

Under the reevaluation program described in Updated Final Safety Analysis Report (UFSAR) Section 3.10.1.2.3, the adequacy of the single frequency, single axis testing was reviewed. Supplemental test data, both on full cabinet assemblies and components, were obtained that utilized multi-frequency biaxial input motion in accordance with IEEE Standard 344-1975 (Reference 75). A complete review of the control room panels and local instrument panels was performed and qualification upgrade to Reference 75 was achieved (see UFSAR Section 3.10.3.1).

Calculation Modification Record (CMR) 8874 to calculation CE-02-90-15 was completed for mounting ODAs APRM-MON-ODA1, APRM-MON-ODA2, RBM-MON-ODA/A, and RBM-MON-ODA/B on control-room panel E-CP-H13/P603. The ODAs will be installed per design and E-CP-H13/P603 seismic 1 qualification will be maintained. This same CMR also qualified the APRM bypass switch mounting to Seismic 1 requirements.

5.4.6.5 Seismic Qualification Conclusion

The NUMAC modified PRNM panel assemblies are seismically qualified to the CGS site-specific seismic licensing design basis loads. More detailed discussions pertaining to the underlying methodology and results are provided in the seismic qualification report (Reference 73).

5.4.7 Electromagnetic Compatibility (EMC) Qualification

The CGS main control room emissions are below the limits established in RG 1.180 (Reference 76) and EPRI-TR-102323 (Reference 77). The CGS emission levels were obtained using data taking methodologies consistent with MIL-STD-461E (Reference 78) recommended test set-ups for RE101, RE102 and CE101. The EMI mapping was performed in June, 2004. Since June 2004, modifications in CGS have all met the EMC qualification requirements of Reference 76 in accordance with plant procedures. Additionally, the use of portable transceivers is administratively controlled by CGS procedure PPM 1.3.72, Control of Portable RF Transmitting Devices.

Electrical separation is maintained in accordance with CGS Design Specification 201, Electrical Separation Design Requirements. The CGS PRNM design meets the separation requirements of CGS Design Specification 201.

Several test methods were performed on generic PRNM instruments in order to demonstrate that the instruments will not be susceptible to failure under certain electromagnetic conditions and that the new design is compatible with electromagnetic environments where the equipment will be installed. The differences between the CGS instruments and the tested instruments were evaluated and found to have no effect on the EMC qualification levels of the CGS instruments. The new PRNM equipment that will be installed at CGS is electro-magnetically qualified based on specific analysis of requirements and comparisons with generic PRNM components.

The following Tables 5-4 and 5-5 outline the EMC Testing Requirements per Reference 1.

Table 5-4 Susceptibility Requirements

EMC	LTR test	RG 1.180 equivalent	Test Levels
[[			
			]]

Table 5-5 Emissions Requirements

EMI	LTR test	RG 1.180 equivalent	Test Levels
[[			
			]]

5.4.7.1 Analysis of LTR and RG 1.180 EMC requirements for Susceptibility and Emissions

[[

]]

Table 5-6 EMC and EMI Requirements

EMC REQUIREMENTS		
EMC	**Susceptibility Test**	**Analysis**
[[		

EMC REQUIREMENTS		
EMC	**Susceptibility Test**	**Analysis**

EMC REQUIREMENTS		
EMC	**Susceptibility Test**	**Analysis**
		]]
EMI REQUIREMENTS		
EMI	**Emissions Test**	**Emissions Test**
[[		
		]]

Table 5-7 Specific Tests

Test not included in GEH EMC qualification of PRNM instrumentation	Test per RG1.180	Analysis of excluded test
Susceptibility Tests		
[[		]]
Emissions Tests		
[[		

Test not included in GEH EMC qualification of PRNM instrumentation	Test per RG1.180	Analysis of excluded test
		]]

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

Based on CGS analysis of the GEH Qualification Summary, the PRNM components are capable of performing their intended functions within design limits and without degradation when subjected to the EMI conditions as specified in:

- EPRI Report, Guidelines for EMI Testing in Power Plants, EPRI TR-102323, June 1994 (Reference 79),
- EPRI-TR-102348 Revision 1, "Guideline on Licensing Digital Upgrade, per RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Controls," (Reference 80).
- RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Controls (Reference 76).

EMC/Radio Frequency Interference (RFI) analysis results shown in Tables 5-6 and 5-7.

5.4.8 NUMAC Interface Computer

[[

]]

5.4.8.1 NIC Environmental Qualification

[[

]]

5.4.8.2 NIC Seismic Qualification

[[ ]]

5.4.8.3 NIC EMC Qualification

[[

]]

5.4.9 Single Failure within the Environmental Control (Control Room Ventilation) System

Per UFSAR Section 9.5, during emergency condition, control room chilled water or SW is supplied to the air handling units for cooling. The control room can be maintained below 85°F by the control room chilled water, or service water (SW) can be used to maintain less than 104°F (shedding of nonessential loads may be required under some conditions). The environmental qualification temperature limit for control room equipment is 104°F and 85°F equivalent temperature for control room personnel habitability.

5.5 Conclusion

The information provided demonstrates through equipment qualification that the CGS PRNMS meets design-basis and performance criteria when the equipment is exposed to mild environments.

The CGS PRNMS is qualified for the most severe CGS Control Environment to which it may be exposed – the CGS main control room - and is relied upon to perform its safety function for the following environmental stressors: Temperature, Humidity, Pressure, Radiation, EMI/RFI, and Seismic. The information presented shows that for each environmental stressor, the equipment qualification is greater than the associated plant environment.

6. Defense-in-Depth and Diversity

6.1 Introduction

NEDC-33694P (Reference 82) evaluates PRNMS upgrade, using the Acceptance Criteria identified in NRC BTP 7-19 (Reference 83).

6.2 Overview

NEDC-33694 (Reference 82) provides an assessment of diversity and defense-in-depth, using the original LTR (Reference 1). Additionally, this report provides a detailed Diversity and Defense-in-Depth (D3) analysis based on a postulated worst-case CCF in the PRNMS programmable entities, and directly addresses all criteria of Reference 83. The evaluation demonstrates that the plant has the diversity and defense-in-depth to cope with any potential CCF in the programmable entities in the upgrade system.

The PRNM system communications and interfaces are described in Sections 1 and 7. The PRNM system is not credited for any response for Anticipated Transient without Scram (ATWS) (10CFR50.62); therefore, Section 7.8 of Reference 70 does not apply to this upgrade.

6.3 Regulatory Evaluation

The NRC position is documented in the SRM on SECY 93-087, "Policy, Technical and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor Design," with respect to common-mode failure (i.e., common-cause failure (CCF)) in digital systems and defense-in-depth. This position was documented in BTP 7-19 Rev. 6, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer Based Instrumentation and Control Systems." Points 1, 2, and 3 of this position are applicable to digital system modifications for operating plants.

Defense-in-depth and diversity in digital I&C systems is focused on ensuring that the safety functions can be achieved in the event of a postulated CCF and the following regulatory requirements should be considered:

> GDC 22, "Protection System Independence," requires, in part, "that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions not result in loss of the protection function Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function."
>
> GDC 24, "Separation of Protection and Control Systems," requires in part that "[i]nterconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired."
>
> GDC 29, "Protection Against Anticipated Operational Occurrences," requires in part defense against anticipated operational transients "to assure an extremely high probability of accomplishing safety functions."

6.4 Defense-in-Depth and Diversity Evaluation

The CGS PRNM upgrade was evaluated using the Acceptance Criteria identified in NRC BTP 7-19 (Reference 83). The Reference 82 report provides an assessment of diversity and defense-in-depth, using the original LTR (Reference 1). Additionally, this report provides a detailed Diversity and D3 analysis based on a postulated worst-case CCF in the PRNMS programmable entities, and directly addresses all criteria of Reference 83. The evaluations demonstrate that the plant has the diversity and defense-in-depth to cope with any potential CCF in the programmable entities in the upgrade system.

7. Communications

7.1 Introduction

NEDC-33697P (Reference 84) addresses the Communications for NUMAC PRNM as specifically configured for ENW's CGS.

7.2 Overview

NEDC-33697P (Reference 84), Section 2, provides a summary description and overview of the CGS PRNM data communication links and pathways. As noted within that overview, detailed descriptions of each of these pathways are provided in the NEDC-33696P (Reference 4). Additionally, communication independence as related to the requirements of IEEE Standard 603 (Reference 71) Clause 5.6 is addressed in Section 9.2.6.

7.3 Regulatory Evaluation

IEEE Standard 603-1991 Clause 5.6, "Independence," requires independence between (1) redundant portions of a safety system, (2) safety systems and the effects of design basis events, and (3) safety systems and other systems. SRP, Chapter 7, Appendix 7.1-C, Section 5.6 "Independence" provides acceptance criteria for this requirement, and among other guidance, provides additional acceptance criteria for communications independence. Section 5.6 states that where data communication exists between different portions of a safety system, the analysis should confirm that a logical or software malfunction in one portion cannot affect the safety functions of the redundant portions, and that if a digital computer system used in a safety system is connected to a digital computer system used in a non-safety system, a logical or software malfunction of the non-safety system should not be able to affect the functions of the safety system.

IEEE Standard 7-4.3.2-2003, endorsed by Regulatory Guide 1.152 Revision 2, Clause 5.6, "Independence," provided guidance on how IEEE Standard 603 requirements can be met by digital systems. This clause of IEEE Standard 7-4.3.2 specifies that, in addition to the requirements of IEEE Standard 603-1991, data communication between safety channels or between safety and non-safety systems not inhibit the performance of the safety function. SRP, Chapter 7, Appendix 7.1-D, Section 5.6, "Independence" provides acceptance criteria for equipment qualifications. This section, 10 CFR Appendix A, GDC 24, "Separation of protection and control systems," states that "the protection system be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel that is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system, and that interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired."

BTP 7-11 provides guidance for the application and qualification of isolation devices. BTP 7-11 applies to the use of electrical isolation devices to allow connections between redundant portions

of safety systems or between safety and non-safety systems. Therefore, this SE only considers applicability between safety and non-safety systems.

SRP Section 7.9, "Data Communications Systems," also contains guidance for data communication systems.

Additional Guidance on interdivisional communications is contained in DI&C-ISG-04 Revision 1, "Highly-Integrated Control Rooms – Communication Issues," (ADAMS Accession No. ML083310185).

7.4 Communications Evaluation

NEDC-33697P (Reference 84) addresses D.7.2 of Reference 15 and identifies the individual documents/sections which provide detailed descriptions/information on the communications configured for ENW's CGS. The DI&C-ISG-04 (Reference 13) Compliance is included as Enclosure 1 of NEDC-33697P (Reference 84).

8. System, Hardware, Software, and Methodology Modifications

8.1 Introduction

NEDC-33697P (Reference 84) addresses the System, Hardware, Software, and Methodology Modifications for NUMAC PRNM as specifically configured for ENW's CGS.

8.2 Overview

NEDC-33697P (Reference 84), Section 3, provides the deviations from the previously the approved LTR and changes made to the original design (Hatch, 1997) that appear in the CGS platform.

8.3 Regulatory Evaluation

The basis on which the new system, hardware, software, or design lifecycle methodology should be evaluated may be the same as the evaluation of the original version of that item; for example, having one component in a system that is environmentally qualified to a higher standard than all of the other components does not appreciably increase the reliability of the system. The various acceptance criteria are discussed throughout ISG-06.

8.4 System, Hardware, Software, and Methodology Modifications Evaluation

The CGS PRNM system has been designed in accordance with the previously approved LTR (Reference 1). The LTR is the base document from which deviations are identified. The CGS PRNM system contains three deviations from the LTR that are evaluated in Enclosure 1 of Reference 14. Changes made to the original design (Hatch in 1997) that appear in the CGS platform are provided in Enclosure 2 of NEDC-33697P (Reference 84).

9. Compliance with IEEE Standard 603

This License Amendment Request includes ARTS/MELLLA changes, as well as a digital upgrade for the PRNM system. The changes for ARTS/MELLLA implementation are justified within NEDC-33507P (Reference 85), and are considered separately from the PRNM system digital upgrade. IEEE Standard 603 (Reference 71) only applies to the digital upgrade; therefore, the ARTS/MELLLA changes are not addressed in the following sub-sections.

9.1 Regulatory Evaluation

For nuclear plants with construction permits issued before January 1, 1971, 10 CFR 50.55a(h) requires that protection systems must be consistent with their licensing basis or may meet the requirements of IEEE Standard 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995. For nuclear power plants with construction permits issued after January 1, 1971, but before May 13, 1999, 10 CFR 50.55a(h) requires that protection systems must meet the requirements stated in either IEEE Standard 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations," or IEEE Standard 603-1991 and the correction sheet dated January 30, 1995. Applications filed on or after May 13, 1999 for construction permits and operating licenses, must meet the requirements for safety systems in IEEE Standard 603-1991 and the correction sheet dated January 30, 1995. SRP Appendix 7.1-C contains guidance for the evaluation of conformance to IEEE Standard 603-1991.

10 CFR 50.55a(a)(3)(i) allows licensees to propose alternatives to paragraph (h), amongst others, provided that the proposed alternative would provide an acceptable level of quality and safety. Where a licensee wishes to demonstrate compliance with another standard in lieu of IEEE Standard 603-1991, including a later edition of IEEE 603 (e.g., the 1998 edition), a request to use a proposed alternative must be submitted with the digital I&C Licensee Amendment Request (LAR). This request must justify why, and the NRC staff must be able to conclude that, meeting the alternate standard provides an equivalent level quality and safety as meeting IEEE Standard 603-1991. The additional review time and effort to approve the alternative (per LIC-102, "Relief Request Reviews" – ML091380595) should depend on how different the alternate standard is from IEEE Standard 603-1991.

9.1 IEEE Standard 603, Clause 4, Design Basis

Requirement: *A specific basis shall be established for the design of each safety system of the nuclear power generating station. The design basis shall also be available as needed to facilitate the determination of the adequacy of the safety system, including design changes.*

The PRNM system upgrade only affects a very small portion of the RPS, and the design basis is unchanged from that of the existing PRM system. The details of the design basis for the PRNM system are provided in the various sections of this document.

9.2 IEEE Standard 603, Clause 5, System

Requirement: *The safety systems shall, with precision and reliability, maintain plant parameters within acceptable limits established for each design basis event. The power, instrumentation, and control portions of each safety system shall be comprised of more than one safety group of which any one safety group can accomplish the safety function. (See Appendix A for an illustrative example.)*

Section 1 of this document describes the overall PRNM system, to the block diagram level. NEDC-33697P (Reference 84) addresses the independence of the power, I&C portions of the safety systems, showing 4 independent channels through the APRM outputs. Per Section 3.2.2 of Reference 1, the number of trip outputs from an APRM channel is one each. The outputs from all four APRM channels go to four independent 2-Out-Of-4 voter channels, two providing inputs to each RPS trip system. In this configuration, output trips from any two or more APRM channels out of four (out of remaining three if one channel is bypassed) will result in a trip output from all four voter channels. This will in turn result in trip signals to each RPS trip system (full scram).

Per Section 8.3.6 of Reference 1, accuracy and drift performance is improved for the PRNM system, as compared to the current PRM system. Per Section 3.4.7 of the NRC SE (Reference 2), the PRNM system is designed to maintain all existing system functions with a level of reliability equal to or better than that assumed in plant safety analyses. Setpoints are either maintained or changed only to take advantage of improved performance characteristics while maintaining existing safety margins.

Section D.9.4.2 of DI&C-ISG-06 (Reference 15) mentions requirements traceability in addressing IEEE Standard 603 (Reference 71), but mentions this as a Phase 2 activity. Therefore, requirements traceability will be addressed within Phase 2.

9.2.1 IEEE Standard 603, Clause 5.1, Single Failure Criterion

Requirement: *The safety systems shall perform all safety functions required for a design basis event in the presence of:*

(1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures;

(2) all failures caused by the single failure; and

(3) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions.

The single-failure criterion applies to the safety systems whether control is by automatic or manual means. IEEE Standard 379-1988 provides guidance on the application of the single-failure criterion.

This criterion does not invoke coincidence (or multiple-channel) logic within a safety group; however, the application of coincidence logic may evolve from other criteria or considerations to maximize plant availability or reliability. An evaluation has been performed and documented in

other standards to show that certain fluid system failures need not be considered in the application of this criterion. The performance of a probabilistic assessment of the safety systems may be used to demonstrate that certain postulated failures need not be considered in the application of the criterion. A probabilistic assessment is intended to eliminate consideration of events and failures that are not credible; it shall not be used in lieu of the single-failure criterion. IEEE Standard 352-1987 and IEEE Standard 577-1976 provide guidance for reliability analysis.

Where reasonable indication exists that a design that meets the single-failure criterion may not satisfy all the reliability requirements specified in 4.9 of the design basis, a probabilistic assessment of the safety system shall be performed. The assessment shall not be limited to single failures. If the assessment shows that the design basis requirements are not met, design features shall be provided or corrective modifications shall be made to ensure that the system meets the specified reliability requirements.

The NRC staff evaluated and approved the single failure proof design of the PRNM system, as described and supplemented in the LTR (Reference 1), based on IEEE Standard 279-1971(Reference 86) Clause 4.2, as discussed in Section 4.4.1.1.2 of the LTR (Reference 1). The failure analysis for the PRNM system is provided in Section 6 of Volume 1 of the LTR (Reference 1(a)) and in Appendix F of Volume 2 of the LTR (Reference 1(b)). Per Section 3.1 of the NRC SE (Reference 2), the NRC staff found that the "combination of architecture, wiring practices, and use of isolation devices provides the required isolation and physical independence to ensure acceptable defense against single failures." The existing four channel recirculation flow processing system is retained. Therefore, the CGS PRNM system is not subject to the potential single failure vulnerability described in Section 4.4.1.1.2 of the Reference 1.

The PRNM system design meets the single failure criteria and the reliability requirements; thus, no probabilistic assessment of the safety system is required.

9.2.2 IEEE Standard 603, Clause 5.2, Completion of Protective Action

Requirement: *The safety systems shall be designed so that, once initiated automatically or manually, the intended sequence of protective actions of the execute features shall continue until completion. Deliberate operator action shall be required to return the safety systems to normal. This requirement shall not preclude the use of equipment protective devices identified in 4.11 of the design basis or the provision for deliberate operator interventions. Seal-in of individual channels is not required.*

As stated in Section 4.4.1.1.16 of (Reference 1, in response to Clause 4.16 of Reference 86, [[

]]

9.2.3 IEEE Standard 603, Clause 5.3, Quality

Requirement: *Components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. Safety system equipment shall be designed,*

manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program (ANSI/ASME NQA1-1989).

Per Section 3.2.4 and Table 3.2-1 of the CGS UFSAR, the RPS and NMS are quality class 1 and meet the requirements of 10 CFR 50 Appendix B.

Utility Quality Assurance Program Information:

Section 9.1.3 of Reference 14 provides specific information regarding the CGS Quality Assurance program for this project.

GEH Quality Assurance Program Information:

Per Section 4.4.1.1.3 of Reference 1, [[

]]

Section 9 of Reference 1 describes special quality program aspects related to the programmable digital NUMAC equipment. Per Section 9.2.1 of Reference 1, [[

]]

Per the NRC SE (Reference 2) for Reference 1, the major components of the PRNM system that must function to perform the system safety functions are the APRM/LPRM chassis, APRM interface panels, voters, Class 1E power supplies, and APRM/OPRM software. These components are safety-related. The LPRM detectors, the recirculation flow detectors, and the associated signal cables from these detectors to the APRM chassis are the same non-safety-related equipment as currently installed in CGS. This equipment will not be replaced in this upgrade, based on nuclear industry reliability experience with this equipment. Additionally, GE uses military specification components wherever possible to achieve high reliability and availability. The hardware development process for the CGS PRNM is detailed in Section 2.

The various types of NUMAC equipment in operation at nuclear power plants have components and modules that are similar to the PRNM system. The reported field failure rates support the conclusion that the PRNM system will be highly reliable.

The PRNM system uses microprocessors with software-based functional and display capabilities. The software resides in programmable read-only memory. For the PRNM system, all of the software for the safety-related functions is considered safety-related and receives the same level of V&V effort. The PRNM system is also modularized such that a single failure in the self-test system or on the front panel display and the keyboard panel will not affect the essential measurement and trip functions. The software development process for PRNM system is detailed in Section 4.

Commercial grade dedication for the PRNM system is described in Sections 2, 4 and 10.3.4.2.

9.2.4 IEEE Standard 603, Clause 5.4, Equipment Qualification

Requirement: *Safety system equipment shall be qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that it will be capable of meeting, on a continuing basis, the performance requirements as specified in the design basis. Qualification of Class 1E equipment shall be in accordance with the requirements of IEEE Standard 323-1983 and IEEE Standard 627-1980.*

The PRNM system is qualified by type test and analysis, in accordance with the requirements of IEEE Standard 323-1983 (Reference 87). The PRNM system equipment qualification is detailed in Section 5.

9.2.5 IEEE Standard 603, Clause 5.5, System Integrity

NEDC-33698P (Reference 88) evaluates the PRNMS upgrade, using the Acceptance Criteria identified in IEEE Standard 603-1991 (Reference 71), Clause 5.5, System Integrity. Guidance on the application of this criterion for safety system equipment employing digital computers and software or firmware is found in Reference 45 Clause 5.5 and SRP (Reference 70) Chapter 7, Appendix 7.1-C, Section 5.5. Compliance with the applicable requirements is shown primarily using the original LTR NEDC-32410P-A (Reference 1).

9.2.6 IEEE Standard 603, Clause 5.6 Independence

9.2.6.1 IEEE Standard 603, Clause 5.6.1, Independence Between Redundant Portions of a Safety System

Requirement: *Redundant portions of a safety system provided for a safety function shall be independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function during and following any design basis event requiring that safety function.*

Reference 89 provides the separation analysis for the CGS PRNM system. Per Section 4.4.1.1.6 of Reference 1, [[

]]

The NRC staff evaluated and approved the channel independence of the PRNM system, as described and supplemented in Reference 1, based on IEEE Standard 279-1971 (Reference 86). Per Section 3.5 of the NRC SE (Reference 2), the APRM/OPRM channels are implemented in physically and electrically separate hardware, thus providing channel independence. The design is consistent with the guidance provided in RG 1.75 (Reference 90), and therefore, the NRC staff found the channel independence to be acceptable.

NEDC-33697P (Reference 84) provides a description of the independence of the PRNM system, including a description of the communications. These descriptions establish the fact that the redundant portions of the safety related portions of the CGS PRNM System are independent and

physically separated from each other to the degree necessary to retain the capability to accomplish the safety function during and following any DBE requiring the safety function.

9.2.6.2 IEEE Standard 603, Clause 5.6.2, Independence Between Safety Systems and Effects of Design Basis Event

Requirement: *Safety system equipment required to mitigate the consequences of a specific design basis event shall be independent of, and physically separated from, the effects of the design basis event to the degree necessary to retain the capability to meet the requirements of this standard. Equipment qualification in accordance with 5.4 is one method that can be used to meet this requirement.*

The PRNM system equipment is located in the control room, a mild environment, and is thus isolated from the harsh conditions of the DBEs. Per Section 4.4.1.1.4 of Reference 1, [[

]] Per Section 4.4.1.1.5 of Reference 1, [[

]] Section 5 describes the Equipment Qualification of the PRNM system, which shows the capability of the system to perform as necessary in the required environments.

The NRC staff evaluated and approved the channel independence of the PRNM system, as described and supplemented in Reference 1, based on IEEE Standard 279-1971 (Reference 86). Per Section 3.5 of the NRC SE (Reference 2), Reference 86 requires that channels that provide signals for the same protective function shall be independent and physically separated to decouple the effects of unsafe environmental factors, electric transients, and physical accident consequences documented in the design basis. Channel independence prevents interactions between channels during maintenance operations or in the event of a channel malfunction. RG 1.75 (Reference 90), "Physical Independence of Electric Systems," endorses IEEE Standard 384-1974 (Reference 91), which describes an acceptable method of ensuring that the circuits and electric equipment for systems that perform safety-related functions are physically independent. The APRM/OPRM channels are implemented in physically and electrically separate hardware, thus providing channel independence. The design is consistent with the guidance provided in Reference 90, and therefore, the NRC staff found the channel independence to be acceptable.

NEDC-33697P (Reference 84) provides a description of the independence of the PRNM system, including a description of the communications. These descriptions establish the fact that the safety related portions of the CGS PRNM System required to mitigate the consequences of a specific DBE are independent and physically separated from the effects of the DBE to the degree necessary to retain the capability to meet the requirements of IEEE Standard 603, Clause 5.6.2.

9.2.6.3 IEEE Standard 603, Clause 5.6.3, Independence Between Safety Systems and Other Systems

Requirement: *The safety system design shall be such that credible failures in and consequential actions by other systems, as documented in 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard.*

The only safety system affected by this change is the PRNM, excluding detectors. There are no changes from the current system design regarding conditions causing functional degradation of safety system performance. Special considerations for D3 are fully addressed in NEDC-33694P (Reference 82).

Section 5 describes the Equipment Qualification of the PRNM system, which shows the capability of the system to perform as necessary in the required environments. Reference 89 provides the separation analysis for the CGS PRNM system.

NEDC-33697P (Reference 84) provides a description of the independence of the PRNM system, including a description of the communications. These descriptions, along with Sections 9.2.6.3.1 through 9.2.6.3.3 below, establish the fact that the safety related portions of the CGS PRNM System is designed such that credible failures in and consequential actions by other systems do not prevent the PRNM System from meeting the criteria of Reference 71, Clause 5.6.3.

9.2.6.3.1 IEEE Standard 603, Clause 5.6.3.1, Interconnected Equipment

Requirement:

(1) Classification: Equipment that is used for both safety and non-safety functions shall be classified as part of the safety systems. Isolation devices used to affect a safety system boundary shall be classified as part of the safety system.

(2) Isolation: No credible failure on the non-safety side of an isolation device shall prevent any portion of a safety system from meeting its minimum performance requirements during and following any design basis event requiring that safety function. A failure in an isolation device shall be evaluated in the same manner as a failure of other equipment in a safety system.

Per Section 4.4.1.1.7 of the LTR (Reference 1), [[

]]

Per Section 3.6.1 of the NRC SE (Reference 2), "In the PRNMS design, all interface connections between control and protection systems are made through optic-based isolation devices of the same classification as the protection system. Additionally, all control wiring is separated from protection system wiring via the use of conduits and physical separation. The staff finds the isolation devices acceptable."

Section 4.2.1 of 24A5221 (Reference 48), the NUMAC PRNM system requirements specification, provides the bases for safety classifications for the NUMAC PRNM equipment. NEDC-33697P (Reference 84) provides a description of the independence of the PRNM system, including a description of the communications. These descriptions establish the fact that the equipment used for both safety and non-safety functions in the CGS PRNM System is classified as part of the safety system where applicable, and the isolation devices used for the safety system boundary are classified as part of the safety system. References 48 and 84 indicate that no credible failure on the non-safety side of an isolation device will prevent any portion of the safety system from performing its safety function during and following any DBE requiring the safety function.

9.2.6.3.2 IEEE Standard 603, Clause 5.6.3.2, Equipment in Proximity

Requirement:

(1) Separation: Equipment in other systems that is in physical proximity to safety system equipment, but that is neither an associated circuit nor another Class 1E circuit, shall be physically separated from the safety system equipment to the degree necessary to retain the safety systems' capability to accomplish their safety functions in the event of the failure of non-safety equipment. Physical separation may be achieved by physical barriers or acceptable separation distance. The separation of Class 1E equipment shall be in accordance with the requirements of IEEE Standard 384-1981.

(2) Barriers: Physical barriers used to effect a safety system boundary shall meet the requirements of 5.3, 5.4 and 5.5 for the applicable conditions specified in 4.7 and 4.8 of the design basis.

The PRNM system components will be mounted in the same cabinets as the existing PRM equipment. Therefore, there will be no change in separation from equipment in other systems from the existing configuration with the PRM. Per Reference 89, the CGS NUMAC PRNM system equipment supplied as a part of this change meets the requirements of References 91 and 92. Per Section 2.1 of Reference 48, the NUMAC PRNM system supplied as a part of this change also meets the requirements of IEEE Standard 384-1992 (Reference 93).

Reference 89 provides the separation analysis for the CGS PRNM system. NEDC-33697P (Reference 84) provides a description of the independence of the PRNM system.

Per the discussion above, the equipment used in other systems that are in physical proximity to CGS PRNM system that is neither an associated circuit nor another Class 1E circuit is physically separated from the safety system equipment to the degree necessary to retain the capability of the PRNM system to accomplish its safety function in the event of the failure of non-safety equipment.

9.2.6.3.3 IEEE Standard 603, Clause 5.6.3.3, Effects of a Single Random Failure

Requirement: *Where a single random failure in a non-safety system can (1) result in a design basis event, and (2) also prevent proper action of a portion of the safety system designed to protect against that event, the remaining portions of the safety system shall be capable of*

providing the safety function even when degraded by any separate single failure. See IEEE Standard 379-1988 for the application of this requirement.

Per Section 3.6.2 of the NRC SE (Reference 2), "PRNMS self-checking features ensure that signals transmitted to non-safety control systems do not cause control system actions that challenge the safety system. Additionally, PRNMS self-testing features ensure that a failed channel will result in either an alarm or a trip of the associated APRM, OPRM, or voter channel. Failure of an APRM or OPRM channel results in an alarm or trip in each voter channel. Failure of a voter channel results in an alarm or a half trip in the RPS, depending on the failure. Because the voter channels cannot be placed in bypass, a second random failure in the voters will not degrade the voter function such that a reactor trip will not occur. The staff finds that these design features satisfy the single random failure criterion regarding channel failures and interactions with control systems."

"A single switch is used to bypass an APRM/OPRM channel. The bypass switch has mutually exclusive positions, thus assuring that only one APRM/OPRM channel is bypassed at a time. Removing an APRM/OPRM channel from service without using the bypass feature will actuate a reactor trip signal for the associated channel. The voter channels cannot be bypassed. Removing a voter channel from service will actuate a reactor trip signal for the associated RPS division. The staff finds that these design features provide adequate redundancy and, therefore, satisfy the single random failure criterion regarding channel bypasses and removal of a channel from service for test or maintenance."

Per Section 3.6.3 of the NRC SE (Reference 2), "The PRNMS is designed to detect events requiring protective functions and limit the consequences of such an event. The original analysis for separation of control and protection equipment remains valid for the APRM and OPRM trip functions in the modified PRNMS, because the PRNMS design uses alternate channels to ensure RPS actuation, and uses diverse algorithms to detect reactor power instabilities. The staff, therefore, finds that the PRNMS design acceptably addresses multiple failures resulting from a credible single event."

Reference 89 provides the separation analysis for the CGS PRNM system. NEDC-33697P (Reference 84) provides a description of the independence of the PRNM system, including a description of the communications. These documents show that non-safety systems are isolated from the PRNM system, such that failures of non-safety systems do not degrade the capability of the PRNM system to perform the required safety functions. Thus, as related to the PRNM system, there are no single random failures in non-safety systems that can (1) result in a DBE, and (2) also prevent proper action of a portion of the safety system (PRNM) designed to protect against that event. Thus, the single failure analysis is still applicable to the PRNM system, as described in Section 9.2.1. The PRNM system is capable of providing the safety function, considering any separate single random failure in a non-safety system.

9.2.6.4 IEEE Standard 603, Clause 5.6.4, Detailed Criteria

Requirement: *IEEE Standard 384-1981 provides detailed criteria for the independence of Class 1E equipment and circuits.*

Per Reference 46, the CGS NUMAC PRNM system equipment supplied as a part of this change meets the requirements of References 91 and 92. Per Section 2.1 of Reference 48, the NUMAC PRNM system supplied as a part of this change also meets the requirements of Reference 93.

Per Section 3.5 of the NRC SE (Reference 2) to the LTR (Reference 1), RG 1.75 (Reference 90) endorses IEEE Standard 384-1974 (Reference 91), which describes an acceptable method of ensuring that the circuits and electric equipment for systems that perform safety-related functions are physically independent. The APRM/OPRM channels are implemented in physically and electrically separate hardware, thus providing channel independence. The design is consistent with the guidance provided in Reference 90. Thus, the NRC staff found the channel independence for the PRNM system to be acceptable.

9.2.7 IEEE Standard 603, Clause 5.7, Capability for Test and Calibration

NEDC-33698P (Reference 88) evaluates the Power Range Neutron Monitoring System (PRNMS) upgrade, using the Acceptance Criteria identified in IEEE Standard 603-1991(Reference 71) Clause 5.7, Capability for Test and Calibration. Guidance on the application of this criterion is found in SRP (Reference 70) Chapter 7, Appendix 7.1-C, Section 5.7. Compliance with the applicable requirements is shown primarily using the original LTR (Reference 1).

9.2.8 IEEE Standard 603, Clause 5.8, Information Displays

9.2.8.1 IEEE Standard 603, Clause 5.8.1, Displays for Manually Controlled Actions

Requirement: *The display instrumentation provided for manually controlled actions for which no automatic control is provided and that are required for the safety systems to accomplish their safety functions shall be part of the safety systems and shall meet the requirements of IEEE Standard 497-1981. The design shall minimize the possibility of ambiguous indications that could be confusing to the operator.*

For the PRNM system, there are no manually controlled actions for which no automatic control is provided that are required for the safety systems to accomplish their safety functions. Thus, this requirement does not apply to this change.

9.2.8.2 IEEE Standard 603, Clause 5.8.2, System Status Indication

Requirement: *Display instrumentation shall provide accurate, complete, and timely information pertinent to safety system status. This information shall include indication and identification of protective actions of the sense and command features and execute features. The design shall minimize the possibility of ambiguous indications that could be confusing to the operator. The display instrumentation provided for safety system status indication need not be part of the safety systems.*

The NRC staff evaluated and approved the PRNM system that is described and supplemented in the LTR, based on IEEE Standard 279-1971 (Reference 86) requirement criteria, as discussed in Section 4.4.1.1.20 of Reference 1. [[

]] The changes to the plant operator's panel will receive human factors reviews per ENW established procedures.

9.2.8.3 IEEE Standard 603, Clause 5.8.3, Indication of Bypasses

Requirement: *If the protective actions of some part of a safety system have been bypassed or deliberately rendered inoperative for any purpose other than an operating bypass, continued indication of this fact for each affected safety group shall be provided in the control room.*

5.8.3.1 This (bypass) display instrumentation need not be part of the safety systems.

5.8.3.2 This indication shall be automatically actuated if the bypass or inoperative condition (a) is expected to occur more frequently than once a year, and (b) is expected to occur when the affected system is required to be operable.

5.8.3.3 The capability shall exist in the control room to manually activate this display indication.

Per Section D.2 of Reference 5, Section 4.2.6.4 of Reference 48, and Section 2.3.1 of References 94 and 95, indication of bypasses is provided for the PRNM system in the control room via indicator lamps, as status lights on the 2-Out-Of-4 voters, and on the headers of the APRM instruments and the ODAs. These indications are activated automatically if an APRM channel is bypassed. The bypass displays, indicator lamps and status lights are continuously active and available to provide indication of bypass when an APRM channel is bypassed.

9.2.8.4 IEEE Standard 603, Clause 5.8.4, Location

Requirement: *Information displays shall be located accessible to the operator. Information displays provided for manually controlled protective actions shall be visible from the location of the controls used to effect the actions.*

Per Section 4.4.1.1.20 of Reference 1 regarding information readout, [[

]]

The NRC staff evaluated and approved the PRNM system that is described and supplemented in the LTR, based on IEEE Standard 279-1971 (Reference 86) requirement criteria, as discussed in Section 4.4.1.1.20 of Reference 1. Per Section 3.19 of the NRC SE (Reference 2), functional information on plant status and equipment status for the PRNMS are available to the operator on the main control panel. Additional equipment status information is available on the PRNM system panel face. The NRC staff found these PRNM system design features acceptable.

9.2.9 IEEE 603, Clause 5.9 Control of Access

Requirement: *The design shall permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof.*

The PRNM safety system equipment is located in the main control room, to which access is controlled by administrative means.

Per Section 4.4.1.1.14 of Reference 1, [[

]]

Per Section 4.4.1.1.18 of Reference 1, regarding trip settings, [[

]]

As stated in Section 3.13 to the NRC SE (Reference 2), the PRNMS has multiple levels of access security, including keylock access and microprocessor-based password protection. Administrative controls and use of a keylock are required to bypass or unbypass a LPRM channel. Additionally, an indicating light on the operator's panel advises the operators that a channel is being accessed. As stated in Section 3.17 to the NRC SE (Reference 2), setpoint adjustments, calibrations, and testing processes are performed using the NUMAC operator interface panel. Access to panel functions is controlled via a keylock on the interface panel and a password for access to software-based settings. User interfaces and controls are described in Section 5.3.18 of the LTR (Reference 1). The NRC staff found these PRNM system design features and administrative control to be acceptable, per the NRC SE (Reference 2).

Details of the security controls, password and keylock access, access to workstations, setpoints, gains, etc., are provided within NEDC-33697P (Reference 84).

9.2.10 IEEE Standard 603, Clause 5.10, Repair

NEDC-33698P (Reference 88) evaluates the Power Range Neutron Monitoring System (PRNMS) upgrade, using the Acceptance Criteria identified in IEEE Standard 603-1991 (Reference 71) Clause 5.10, Repair. Guidance on the application of this criterion for safety system equipment employing digital computers and software or firmware is found in SRP (Reference 70) Chapter 7, Appendix 7.1-C, Sections 5.7 and 6.5. Compliance with the applicable requirements is shown primarily using Reference 1.

9.2.11 IEEE Standard 603, Clause 5.11, Identification

Requirement: *In order to provide assurance that the requirements given in this standard can be applied during the design, construction, maintenance, and operation of the plant, the following requirements shall be met:*

(1) Safety system equipment shall be distinctly identified for each redundant portion of a safety system in accordance with the requirements of IEEE Standard 384-1981 and IEEE Standard 420-1982.

(2) Components or modules mounted in equipment or assemblies that are clearly identified as being in a single redundant portion of a safety system do not themselves require identification.

(3) Identification of safety system equipment shall be distinguishable from any identifying markings placed on equipment for other purposes (for example, identification of fire protection equipment, phase identification of power cables).

(4) Identification of safety system equipment and its divisional assignment shall not require frequent use of reference material.

(5) The associated documentation shall be distinctly identified in accordance with the requirements of IEEE Standard 494-1974.

Per Reference 89, the CGS NUMAC PRNM system equipment will comply with the requirements of Reference 91 and 92 when installed. Per Section 2.1 of Reference 48, the NUMAC PRNM system will also meet the requirements of Reference 93 when installed.

Per Section 3.21 of the NRC SE (Reference 2) for Volume 1 of the LTR, the PRNM system equipment, components, and modules will be mounted in the existing RPS cabinets in the main control room. These cabinets are clearly identified as being in a single redundant portion of the protection system, and, consequently, the PRNM system equipment does not require identification. Because of the cabinet designations, frequent use of reference material is not necessary to identify the equipment or its divisional assignment.

Per Section 4.4.1.1.22 of Reference 1, [[

]] These identifications are distinguishable from identifying markings on equipment for other purposes.

Associated documentation for the equipment is distinctly identified, similar to the existing documentation for the CGS safety systems.

9.2.12 IEEE Standard 603, Clause 5.12, Auxiliary Features

Requirement: *Auxiliary supporting features shall meet all requirements of this standard.*

Requirement: *Other auxiliary features that (1) perform a function that is not required for the safety systems to accomplish their safety functions, and (2) are part of the safety systems by association (that is, not isolated from the safety system) shall be designed to meet those criteria necessary to ensure that these components, equipment, and systems do not degrade the safety systems below an acceptable level. Examples of these other auxiliary features are shown in Figure 3 and an illustration of the application of this criteria is contained in Appendix A [of IEEE Standard 603 1991].*

Auxiliary supporting features are defined by IEEE Standard 603-1991 (Reference 71) as "systems or components that provide services (such as cooling, lubrication, and energy supply) required for the

safety systems to accomplish their safety functions." The PRNM system equipment is considered a direct part of the safety system (RPS), and is treated as such. Thus, the PRNM system equipment has no auxiliary supporting features, as defined. The following paragraph applies if any PRNM system components or functions are interpreted to be "other auxiliary features."

The NRC staff evaluated and approved the PRNM system described and supplemented in Reference 1, based on IEEE Standard 279-1971 (Reference 86) requirement criteria, as discussed in Section 4.4.1 of the LTR. The adequacy of separation and independence are addressed in NEDC-33697P (Reference 84). The PRNM system, including all components, is a single failure proof design, as addressed by Section 9.2.1. Thus, the individual system components and equipment (safety and non-safety) do not degrade the safety systems below acceptable levels.

9.2.13 IEEE Standard 603, Clause 5.13, Multi-Unit Stations

Requirement: *The sharing of structures, systems, and components between units at multi-unit generating stations is permissible provided that the ability to simultaneously perform required safety functions in all units is not impaired. Guidance on the sharing of electrical power systems between units is contained in IEEE Standard 308-1980. Guidance on the application of the single failure criterion to shared systems is contained in IEEE Standard 379-1988.*

The RPS is not a shared system for multiple units. Therefore, this requirement does not apply to the PRNM system.

9.2.14 IEEE Standard 603, Clause 5.14, Human Factors Considerations

Requirement: *Human factors shall be considered at the initial stages and throughout the design process to assure that the functions allocated in whole or in part to the human operator(s) and maintainer(s) can be successfully accomplished to meet the safety system design goals, in accordance with IEEE Standard 1023-1988.*

Per Section 4.4.1.9 of Reference 1, the design of the PRNM system replacement equipment meets the intent of NUREG-0700 (Reference 96) as applicable to the back panel equipment. The base design for the plant operator's panel uses the existing operator interface devices, so there is no effect on the plant human factors evaluations. The digital NUMAC Operator's Display Assembly alternate for the plant operator's panel display has been designed to meet Reference 96 to the extent applicable.

Per Section G.1 of Volume 2 of the LTR (Reference 1(b)), [[

]]

Per Section 3.19 of the NRC SE (Reference 2), functional information on plant status and equipment status for the PRNMS are available to the operator on the main control panel. Additional equipment status information is available on the PRNM system panel face. In addition, status indication for the

OPRM functions will be added to the operator control panel. The NRC staff found these PRNM system design features acceptable.

The site design change process requires performing a Human Factors Engineering (HFE) review of changes to the Control Room Operator's panels, in accordance with NUREG 0700 (Reference 96). The HFE evaluation is provided in the CGS LAR Enclosure 2, Section 2.1.2, Item 6.

9.2.15 IEEE Standard 603, Clause 5.15, Reliability

Requirement: *For those systems for which either quantitative or qualitative reliability goals have been established, appropriate analysis of the design shall be performed in order to confirm that such goals have been achieved. IEEE Standard 352-1987 and IEEE Standard 577-1976 provide guidance for reliability analysis.*

Per Enclosure B of DI&C-ISG-06 (Reference 15), the reliability analysis is to be supplied with the Phase 2 LAR, and will not be provided herein. The reliability analysis methodology will be consistent with that described in Section 6 of the LTR (Reference 1) as modified by LTR Supplement 1 (Reference 1(c)). The reliability analysis will provide the basis for concluding that Section 5.3.14 of the LTR (Reference 1) remains valid for the CGS PRNM system. [[

]]

9.3 IEEE Standard 603, Clause 6, Sense and Command Features

Requirement: *In addition to the functional and design requirements in Section 5, the following requirements shall apply to the sense and command features:*

Per Section 2 of IEEE Standard 603-1991 (Reference 71), "sense and command features" are defined as, "The electrical and mechanical components and interconnections involved in generating those signals associated directly or indirectly with the safety functions. The scope of the sense and command features extends from the measured process variables to the execute features input terminals."

The PRNM system upgrade generally replaces only portions the sense and command features. For conservatism, the sense and command features requirements will be applied to the parts of the replacement PRNM system associated directly or indirectly with safety functions. The sensors are not to be replaced per this upgrade.

9.3.1 IEEE Standard 603, Clause 6.1, Automatic Control

Requirement: *Means shall be provided to automatically initiate and control all protective actions except as justified in 4.5. The safety system design shall be such that the operator is not required to take any action prior to the time and plant conditions specified in 4.5 following the onset of each design basis event. At the option of the safety system designer, means may be provided to automatically initiate and control those protective actions of 4.5.*

A description of the operation of the PRNM is included in Section 1.1. Per Section 3.3.2 of Reference 1(a), the safety functions of the PRNM system are:

- APRM Neutron Flux -- High Trip
- APRM STP -- High Trip
- APRM Neutron Flux -- High (Setdown) Trip
- OPRM Instability Detect-and-Suppress Trip

As shown by Section 4.4.1.1.16 of Reference 1(a), the protective actions of the system are the RPS trips. The PRNM system safety functions are fully automatic, with no operator action required. The APRM and OPRM reactor trip functions automatically initiate the RPS, which is carried through to completion with no operator action required.

9.3.2 IEEE Standard 603, Clause 6.2, Manual Control

9.3.2.1 IEEE Standard 603, Clause 6.2.1, Manual Control

Requirement: *Means shall be provided in the control room to implement manual initiation at the division level of the automatically initiated protective actions. The means provided shall minimize the number of discrete operator manipulations and shall depend on the operation of a minimum of equipment consistent with the constraints of 5.6.1.*

The PRNM system equipment, components, and modules will be mounted in the existing RPS cabinets in the main control room and all PRNM system interfaces will be solely located in the Main Control Room at CGS. The APRM/OPRM bypass switch will be located on panel H13-P603 in the "Operator-at-the-Controls zone" within the main control room.

Per Section 4.4.1.1.17 of Reference 1(a), means are provided to manually actuate the APRM or OPRM trip outputs to the 2-Out-Of-4 voting logic, or the direct inputs to the RPS from the 2-Out-Of-4 Logic Module (output of the 2-Out-Of-4 voting logic). This capability would normally be used only in the event of loss of more than the allowed number of APRM/OPRM or voter channels, resulting in the need for action in accordance with TS.

Additionally, manual scram capability is maintained for RPS, and is unaffected by this upgrade.

Per Section 3.16 of the SER (Reference 2) for the LTR, the NRC staff evaluated and approved the PRNM system design with regard to Manual Control, based on IEEE Standard 279-1971 (Reference 86, par. 4.17) requirement criteria.

9.3.2.2 IEEE Standard 603, Clause 6.2.2, Manual Control

Requirement: *Means shall be provided in the control room to implement manual initiation and control of the protective actions identified in 4.5 that have not been selected for automatic control under 6.1. The displays provided for these actions shall meet the requirements of 5.8.1.*

The design of the NUMAC PRNM does not require or rely on manual initiation or control of any protective actions. There is no manual initiation of protective actions, other than manual actuation of an APRM as described in Section 9.3.2.1.

Refer to NEDC-33696 (Reference 4) for a detailed discussion on operator controls for manual initiation of protective actions and information displays.

This criterion is not applicable to the PRNM system upgrade. Per Section 3.16 of the SER (Reference 2) for the LTR, the NRC staff evaluated and approved the PRNM system design with regard to Manual Control, based on IEEE Standard 279-1971 (par. 4.17) requirement criteria, as described in Section 4.4 of the LTR (Reference 1(a)).

9.3.2.3 IEEE Standard 603, Clause 6.2.3, Manual Control

Requirement: *Means shall be provided to implement the manual actions necessary to maintain safe conditions after the protective actions are completed as specified in 4.10. The information provided to the operators, the actions required of these operators, and the quantity and location of associated displays and controls shall be appropriate for the time period within which the actions shall be accomplished and the number of available qualified operators. Such displays and controls shall be located in areas that are accessible, located in an environment suitable for the operator, and suitably arranged for operator surveillance and action.*

Per Section 4.4.1.1.20 of Reference 1(a), the information available to the operator regarding functional and equipment status remains unchanged by the PRNM modification. Additional equipment status information is available to the plant operator as diagnostic information on user request, but does not change the basic operational information.

Per Sections 3.18, 3.19 and 3.21 of the SER (Reference 2), the PRNM system equipment, components, and modules will be mounted in the existing RPS cabinets in the main control room. Functional information on plant status and equipment status for the PRNM system is available to the operator on the main control panel. Additional equipment status information is available on the PRNM system panel face. APRM and OPRM channel trips and alarms are indicated on the operator's control panel.

Refer to (NEDC-33696 (Reference 4) for a detailed discussion on operator manual controls and information displays.

The NRC staff evaluated and approved the PRNM system design with regard to operator controls and information displays (Section 3.18, 3.19 and 3.21 of the SER (Reference 2), based on IEEE Standard 279-1971 (Reference 86, par. 4.20) requirement criteria, as described in Section 4.4 of the LTR (Reference 1(a)). The PRNM system to be installed at CGS does not include any plant-specific changes that would invalidate this conclusion.

9.3.3 IEEE Standard 603, Clause 6.3, Interaction with Other Systems

Requirement:

6.3.1 Where a single credible event, including all direct and consequential results of that event, can cause a non-safety system action that results in a condition requiring protective action and can concurrently prevent the protective action in those sense and command feature channels designated to provide principal protection against the condition, one of the following requirements shall be met:

(1) Alternate channels not subject to failure resulting from the same single event shall be provided to limit the consequences of this event to a value specified by the design basis. Alternate channels shall be selected from the following:

(a) Channels that sense a set of variables different from the principal channels.

(b) Channels that use equipment different from that of the principal channels to sense the same variable.

(c) Channels that sense a set of variables different from those of the principal channels using equipment different from that of the principal channels.

Both the principal and alternate channels shall be part of the sense and command features.

(2) Equipment not subject to failure caused by the same single credible event shall be provided to detect the event and limit the consequences to a value specified by the design bases. Such equipment is considered a part of the safety system.

See Figure 5 (of IEEE Standard 603 1991) for a decision chart for applying the requirements of this section.

6.3.2 Provisions shall be included so that the requirements in 6.3.1 can be met in conjunction with the requirements of 6.7 if a channel is in maintenance bypass. These provisions include reducing the required coincidence, defeating the non-safety system signals taken from the redundant channels, or initiating a protective action from the bypassed channel.

Per Section 4.4.1.7 of Reference 1(a), the original analysis for separation of control and protection equipment for the APRM (with the current PRM) remains valid for the APRM and OPRM trip functions in the PRNM. All interface connections with control hardware in the PRNM are made through devices providing isolation equal to or better than the current system. All control wiring is separated from protection system wiring. Bypass connections which were isolated through relays providing "exclusive or" logic in the current APRM system are made entirely with fiber-optic connections in the PRNM.

Additionally, the PRNM system design meets the single failure criteria, with full consideration of maintenance bypass operation, as described further in Section 9.2.1. PRNM system communications and isolation are described in detail in the NEDC-33697 (Reference 84).

Per Sections 4.4.1.1.1 and 4.4.1.1.2 of Reference 1(a), bypass of APRM/OPRM channels is accomplished with a single mechanical/optical switch with mutually exclusive positions. All communications paths to and from the switch, and to the 2-Out-Of-4 voter channels is via fiber-optic links using dynamic signals. The final separate check of the signals, performed independently by each voter channel assures that no single failure will cause an inadvertent bypass. When a bypass is active, the input from the bypassed APRM/OPRM channel (APRM or OPRM trip function) will be bypassed by removing it from the vote. The remaining signals are voted with a 2-out-of-3 logic, thus retaining the ability to withstand a single channel failure.

The PRNM system is designed to allow one APRM/OPRM channel, but no voter channels, to be bypassed. A trip from any one unbypassed APRM or OPRM function will result in a "half-trip" in all

four of the voter channels, but no trip inputs to either RPS trip system. A trip from any two unbypassed APRM or OPRM channels will result in a full trip in each of the four voter channels, which in turn results in two trip inputs into each RPS trip system. Three of the four APRM / OPRM channels and all four of the voter channels are required to be operable to ensure that no single instrument failure will preclude a scram from this function on a valid signal.

The NRC staff evaluated and approved the PRNM system design with regard to multiple failures resulting from a credible single event, via Section 3.6.3 of the SER (Reference 2), based on PRNM system compliance with IEEE Standard 279-1971 (Reference 86) requirement criteria (paragraph 4.7), as described in Sections 4.4, 5.3, 6.2, 6.3 and 6.4 of the LTR (Reference 1(a)). The PRNM system is designed to detect events requiring protective functions and limit the consequences of such an event. The original analysis for separation of control and protection equipment remains valid for the APRM and OPRM trip functions in the modified PRNM system, because the PRNM system design uses alternate channels to ensure RPS actuation, and uses diverse algorithms to detect reactor power instabilities. The PRNM system to be installed at CGS does not include any plant-specific changes that would invalidate these conclusions. Therefore, there are no credible events, including all direct and consequential results, which could cause a non-safety system action that results in a condition requiring protective action and can concurrently prevent the required protective action from the PRNM system.

9.3.4 IEEE 603, Clause 6.4, Derivation of System Inputs

Requirement: *To the extent feasible and practical, sense and command feature inputs shall be derived from signals that are direct measures of the desired variables as specified in the design basis.*

Per Section 4.4.1.1.8 of Reference 1(a), the original analysis for the APRM applies for the APRM and OPRM trip functions in the PRNM. The PRNM system directly measures neutron flux via the LPRMs, with no change to scaling, to determine and protect against a reactor over-power condition. The original analysis for the bypass function applies except that the PRNM bypass is derived from only one control room "joystick" switch in the PRNM (one APRM/OPRM channel bypass out of four total) compared to two for the current system (one APRM channel bypass in each RPS trip system). Per Section 5.3.17 of Reference 1(a), the PRNM system also receives eight recirculation loop flow signals (unchanged from the original PRM condition); four from loop A and four from loop B. One signal from each loop goes into each of four PRNM APRM channels.

The NRC staff evaluated and approved the PRNM system design with regard to derivation of system inputs in Section 3.7 of the SER (Reference 2), based on PRNM system compliance with IEEE Standard 279-1971 (Reference 86) requirement criteria (paragraph 4.8), as described in Sections 4.4 and 5 of the LTR (Reference 1(a)). The PRNM system to be installed at CGS does not include any plant-specific changes that would invalidate these conclusions.

9.3.5 IEEE 603, Clause 6.5, Capability for Testing and Calibration

Requirement:

6.5.1 Means shall be provided for checking, with a high degree of confidence, the operational availability of each sense and command feature input sensor required for a safety function during reactor operation. This may be accomplished in various ways; for example:

(1) by perturbing the monitored variable,

(2) within the constraints of 6.6, by introducing and varying, as appropriate, a substitute input to the sensor of the same nature as the measured variable, or

(3) by cross-checking between channels that bear a known relationship to each other and that have readouts available.

Per Section 4.4.1.1.9 of Reference 1(a), the sensor check capability for LPRM detectors remains unchanged from the current system and applies both for the APRM and OPRM trip functions. The check of the bypass input is similar to the current system except that observation of correct response is made at the 2-Out-Of-4 Logic Module display in the PRNM.

As documented in CGS LAR (Enclosure 1, Section 2.2.3.1), the revised TS, updated for the PRNM system modification, include channel checks for the following equipment at a required performance frequency as noted in Table 9.3.5-1.

Table 9.3.5-1 Technical Specification Surveillance – APRM Channel Check

TS / Function	SR	Frequency
RPS Instrumentation 3.3.1.1 Table 3.3.1.1-1.2 Average Power Range Monitors		
2.a Neutron Flux High (Setdown)	3.3.1.1.1	12 hours
2.b STP - High		
2.c Neutron Flux High		
2.e 2-Out-Of-4 Voter[1]		
2.f OPRM Upscale[1]		

[1]New requirement

Refer to Section 3 of NEDC-33698 (Reference 88) for a detailed discussion on PRNM system testing and calibration features, including sensor checks and channel checks.

The NRC staff evaluated and approved the PRNM system design with regard to checking the operational availability of each sense and command feature input sensor required for a safety function during reactor operation in Section 3.8 of the SER (Reference 2), based on PRNM system compliance with IEEE Standard 279-1971 (Reference 86) requirement criteria (paragraph 4.9), as described in Section 4.4 and Section 5 of the LTR (Reference 1(a)). Per Section 3.8 of the SER (Reference 2), the sensor check capability for the LPRM detectors and the recirculation flow rates remains the same with the PRNM system, as now exists in operating BWRs. The PRNM system to be installed at CGS does not include any plant-specific changes that would invalidate these conclusions.

Requirement:

6.5.2 One of the following means shall be provided for assuring the operational availability of each sense and command feature required during the post-accident period:

(1) Checking the operational availability of sensors by use of the methods described in 6.5.1,

(2) Specifying equipment that is stable and retains its calibration during the post-accident time period.

The operational availability of sensors is verified by both automatic self-testing and by channel checks performed on a 12-hour basis per the TS, as shown above.

Per Section 4.1.1.4 of Reference 5, data received from other plant systems which, by nature of their content, have the potential for causing a PRNM safety function to be performed in a non-conservative manner shall be validated prior to its use. The different types of validation checks that shall be performed, depending upon the type of data, are as follows:

- Range Check - Signals are range checked to assure they are within their calibrated ranges and out-of-range data is not used.
- Reasonability Check - Signals are checked against other similar signals to determine whether their value is reasonable. Unreasonable values are flagged and not used if reasonable values are available.
- Operator Check - Data is displayed on a screen to be reviewed and accepted by the operator.
- All multiplexed transmissions pass "transmission" validity checks (parity, structure, or similar).
- Critical Signals are dynamically encoded (signal must continue to change a certain way) so that the receiver can take predefined action when the Specific Criteria are not met.

Refer to Section 3 of NEDC-33698 (Reference 88) for a detailed discussion on PRNM system testing and calibration features, including sensor checks.

Per Section 8.3.4.2.3 of Reference 1(a), the NUMAC APRM contains extensive self-testing which will detect most hardware failures with an equivalent surveillance interval of about one hour. Failures that are not directly tested will most likely be detected by the Channel Check which includes monitoring to confirm the self-test function is still operating, but are assumed only to be found as part of the Channel Functional Test. All functions are accomplished using the same hardware and processing paths that are exercised or monitored by self-test, so one set of tests effectively tests all functions. Analog hardware is limited to the initial input devices and is highly reliable with virtually no drift. All processing is digital, so it is very unlikely that a failure will occur that will not be detected by one or more test paths. Built-in hardware monitors the system (dynamic monitoring of CPU output by output modules and by a watchdog timer).

As part of the automatic self-test, the 2-Out-Of-4 voter channels monitor the APRM channel signals to assure they continue to meet dynamic encoding requirements. The signals are processed and returned to one of the APRM channels to provide a "closed loop" monitor of the voter channels. The

combination of the above provides adequate confidence that a sufficient number of channels will either continue to operate between Channel Functional Tests, or that failures will be detected either by the automatic self-test or Channel Checks.

Per Section 4.4.1.1.5 of Reference 1(a), the equipment required to perform the APRM and OPRM trip functions and that necessary to assure no inadvertent bypass, and all associated equipment is designed to operate in both the normal and abnormal plant control room environment, including EMI, under seismic loads. The qualified environmental limits of the PRNM system are encompassed by the plant specific control room environmental limits per Section 5; therefore, the equipment is designed to function in both the normal and post-accident environments of the control room.

Within Section 3.4.7 of the SER (Reference 2), the NRC staff concurred with GE's assertion that the PRNM system is designed to maintain all existing system functions with a level of reliability equal to or better than that assumed in plant safety analyses, based on the proven design and reliability of the NUMAC product line. Setpoints are either maintained or changed only to take advantage of improved performance characteristics while maintaining existing safety margins. System response times are equal to or better than those of the original system. The NRC staff further concurred with GEH's conclusion that there is no effect on the safety analysis report Chapter 15 design basis accident analyses, and conclusions from those analyses remain valid, per Section 3.4.7 of the SER (Reference 2).

As demonstrated in the above discussion and the referenced description and design report, the PRNM system equipment meets IEEE Standard 603 (Reference 71), Clauses 6.5.1 and 6.5.2, Capability for Testing and Calibration, regarding operational availability of sensors and stability and reliability of equipment and its calibration in the post-accident environment.

9.3.6 IEEE 603, Clause 6.6, Operating Bypass

Requirement: *Whenever the applicable permissive conditions are not met, a safety system shall automatically prevent the activation of an operating bypass or initiate the appropriate safety function(s). If plant conditions change so that an activated operating bypass is no longer permissible, the safety system shall automatically accomplish one of the following actions:*

(1) Remove the appropriate active operating bypass(es).

(2) Restore plant conditions so that permissive conditions once again exist.

(3) Initiate the appropriate safety function(s).

As stated in Section 4.4.1.1.12 of Reference 1(a), the original analysis for the PRM applies for the APRM and OPRM trip functions in the PRNM, with respect to operating bypasses. There are no automatic bypasses for the APRM trip function. The OPRM includes "enabling logic" that automatically activates the trip output only in certain operating zones in the power/flow map (nominally above 30% power and below 60% flow). The APRM trip setpoint is automatically changed to a lower value (setdown) when the manually operated reactor mode switch is not in RUN.

The NRC staff evaluated and approved the PRNM system design with regard to operating bypasses in Section 3.11 of the SER (Reference 2). NRC approval of the design was based on PRNM system compliance with IEEE Standard 279-1971 (Reference 86) requirement criteria (paragraph 4.12), as described in Sections 4.4 and 5.3 of the LTR (Reference 1(a)).

9.3.7 IEEE 603, Clause 6.7, Maintenance Bypass

Requirement: *Capability of a safety system to accomplish its safety function shall be retained while sense and command features equipment is in maintenance bypass. During such operation, the sense and command features shall continue to meet the requirements of 5.1 and 6.3.*

EXCEPTION: One-out-of-two portions of the sense and command features are not required to meet 5.1 and 6.3 when one portion is rendered inoperable, provided that acceptable reliability of equipment operation is otherwise demonstrated (that is, that the period allowed for removal from service for maintenance bypass is sufficiently short to have no significantly detrimental effect on overall sense and command features availability).

Per Sections 4.4.1.1.1 and 4.4.1.1.2 of Reference 1(a), bypass of APRM/OPRM channels is accomplished with a single mechanical/optical switch with mutually exclusive positions. All communications paths to and from the switch, and to the 2-Out-Of-4 voter channels is via fiber-optic links using dynamic signals. The final separate check of the signals, performed independently by each voter channel assures that no single failure will cause an inadvertent bypass. When a bypass is active, the input from the bypassed APRM/OPRM channel (APRM or OPRM trip function) will be bypassed by removing it from the vote. The remaining signals are voted with a 2-Out-Of-3 logic, thus retaining the ability to withstand a single channel failure.

The PRNM system is designed to allow one APRM/OPRM channel, but no voter channels, to be bypassed. A trip from any one unbypassed APRM or OPRM function will result in a "half-trip" in all four of the voter channels, but no trip inputs to either RPS trip system. A trip from any two unbypassed APRM or OPRM channels will result in a full trip in each of the four voter channels, which in turn results in two trip inputs into each RPS trip system. Three of the four APRM / OPRM channels and all four of the voter channels are required to be operable to ensure that no single instrument failure will preclude a scram from this function on a valid signal. Thus, the PRNM system meets the single failure criterion of Clause 5.1 of IEEE Standard 603-1991 (Reference 71) with one channel in maintenance bypass(see also Section 9.2.1). See Section 9.3.3 for an explanation of how the requirements of Clause 6.3 of Reference 71 are met with consideration of one channel being in maintenance bypass.

The NRC staff evaluated and approved the PRNM system design with regard to its capability to accomplish its safety function while sense and command features equipment is in maintenance bypass in Section 3.10 of the SER (Reference 2). NRC approval of the design was based on PRNM system compliance with IEEE Standard 279-1971 (Reference 86) requirement criteria (paragraph 4.11), as described in Section 4.4.1.1.11 of the LTR (Reference 1(a)).

9.3.8 IEEE 603, Clause 6.8 Setpoints

Requirement: *The allowance for uncertainties between the process analytical limit documented in Section 4.4 and the device setpoint shall be determined using a documented methodology. Refer to ISA S67.04-1987.*

Where it is necessary to provide multiple setpoints for adequate protection for a particular mode of operation or set of operating conditions, the design shall provide positive means of ensuring that the more restrictive setpoint is used when required. The devices used to prevent improper use of less restrictive setpoints shall be part of the sense and command features.

Setpoint Methodology -- non-OPRM

GEH setpoints are calculated using the NRC approved methodology contained in NEDC-31336P-A (Reference 97). Conceptually, the GEH method is based on Instrument Society of America (ISA) Method 2, but leads to more conservative setpoints and is referred to as "Method 2 plus". According to this NRC approved methodology, the setpoints are calculated from the Analytic Limit (AL), or the Allowable Value (AV) if there is no AL, using a top down approach, and margin is calculated by methodology:

- between the AL and the AV,
- between the AL and the Nominal Trip Setpoint (NTSP), and
- between the AV and the NTSP.

The margin between the AL and the final NTSP is at least equal to, and generally greater than that needed to meet the 95% probability requirement of RG 1.105.

GEH's setpoint methodology for operating plants uses single-sided distributions in the development of AVs and NTSPs for instrument channels that provide trips when the process variable being measured approaches the setpoint in one direction, as described in ISA standard 67.04 part II. Each of the setpoint functions for the CGS and ARTS/MELLLA project provide trips where the setpoint is approached in only one direction. Per the SE from the NRC (dated 6 November 1995) for Reference 97:

> "The GE methodology utilizes single-sided distributions in the development of trip setpoints and allowable values. ... The staff has stated that this methodology is acceptable provided that a channel approaches a trip in only one direction."

GEH's setpoint methodology for operating plants uses vendor instrument error specifications conservatively to provide setpoints that meet margin requirements to a high degree of confidence. This was demonstrated by actual data analysis during licensing of the GEH methodology (Reference 97). The NRC approved GEH's Instrument Setpoint Methodology in November 1995 while RG 1.105 Revision 2 (Reference 98) was in use. RG 1.105 Revision 3 (Reference 99) was introduced in December 1999, but the revised content, that quantified the confidence level to be 95%, did not invalidate or affect the approved GEH Setpoint Methodology. Per the SE from the NRC for Reference 97:

> "... the BWROG presented data to show that although the GE setpoint methodology does not produce results with a defined confidence level, it was shown that the data analysis can produce results that have a high degree of confidence (95 percent confidence limits). ... By establishing that the 95 percent confidence intervals are bounded by the design allowances developed per NEDC-31336, GE has shown that the results produced by the GE setpoint methodology can be established with high confidence."

The AL is a process parameter value used in the safety analysis and represents a limiting value for the automatic initiation of protective actions. From the AL, an AV is first calculated where its margin to the AL is based on all measurement errors except Drift. [[

]]

All random errors are combined using Square Root of the Sum of the Squares (SRSS) method, and non-conservative bias errors are added algebraically. The AV represents the limiting value to which a setpoint can drift (as determined from surveillance) and still assure that the AL is protected. [[

]] The AV is the value specified in the TS, and is an AL surrogate that assures the AL is protected if the setpoint does not exceed it.

[[

]]

Figure 9.3.8-1 GEH Setpoint Methodology

The approved GEH setpoint methodology basically results in two calculated NTSPs as shown in Figure 9.3.8-1. [[

]] NTSP1 is the Limiting Trip Setpoint (LTSP), as the instrument setting can be no closer to the AL than NTSP1. However, NTSP1 generally does not have the margin to the AV required by GEH methodology, and so is seldom the final adjusted NTSP, called **"NTSP (Adj)" (or "$NTSP_F$")**, the second NTSP. An intermediate NTSP, "NTSP2" is also calculated as part of the NTSP (Adj) calculations. [[

]] Relevant equations are shown below. [Notes: $\Re$ refers to the random component for each error. The subscript L refers to the error for the whole instrument loop, and the errors are based on a one-sided approach to the setpoints.]

[[ ]]

AV = AL – AVMARGIN (for an increasing setpoint)

[[ ]]

NTSP1 = AL – NTSP1MARGIN (for an increasing setpoint)
= LTSP

Per NEDC-31336P-A (Reference 97), [[

]] As shown in Figure 9.3.8-1, [[

]] All setpoints are reset to the NTSP(Adj), within the ALT, after calibration. [[

]] (also see the equation below). All LATs are equal to their associated ALTs (the tolerance within which the device calibration reading is left after calibrating). Relevant equations are shown below.

[[ ]] (calculated for each instrument **i** in the instrument loop)

LAT = ALT

The calibration tools and standards uncertainties (errors) are considered within GEH methodology and the values used are identified in the GEH Instrument Limits Calculation(s). These uncertainty values in the calculation bound the tools and standards used for calibration in the field. Calibration tools and standards uncertainties are used within the calculation and they provide the uncertainty boundaries for the use of any new instruments. Otherwise the setpoint calculation would need to be re-calculated using the uncertainties of the new instrument(s) that are outside of the bounding values in the calculation for the calibration tools and standards.

Regarding Calibration conditions, the temperature range for Calibrations is considered in the GEH Setpoint Methodology, as part of the Temperature Effect for the instruments involved. For example, for the calibration of the Recirculation Flow Transmitters, the temperature range for calibration is 70 to 104°F, meaning that the calibration could occur at a different specific temperature each time. The total difference in temperature could be 34°F, and that maximum is applied to the Temperature Effects for the Rosemount 1153 Flow Transmitter instruments in the calculation of instrument errors.
[[ ]]

[[

]] If the AV/NTSP1 margin is not sufficient for the LER avoidance test, the NTSP is conservatively adjusted to provide added margin.

The GEH setpoint methodology performs an additional LAT test to determine if the NTSP needs to be adjusted further in the conservative direction. [[

]]

If the NTSP has sufficient margin to meet these requirements for LAT, no adjustment to NTSP is required. However, if margin is not sufficient, the NTSP is adjusted to provide added margin. This adjusted NTSP is "NTSP(Adj)", and it is also checked for LER avoidance. The NTSP (Adj) is the final NTSP that is set into the instrument loop. After each calibration, the instrument is reset to this final NTSP(Adj), within the ALT.

[[

]]

[[

]] The OL is an operational limit on the opposite side of the setpoint than the AL, and generally represents the parameter value for normal operation.

The Table 9.3.8-1 provides an example of results from a typical setpoint calculation performed using GEH setpoint methodology. The example is for a plant's APRM Neutron Flux Scram setpoint function in units of percent Rated Thermal Power (RTP). Note as stated earlier, the final NTSP (Adj) is further away from the AL than NTSP1, the LTSP.

Table 9.3.8-1 Typical Setpoint Calculation Results

Parameter	% RTP
AL	122
AV	119.3
NTSP1 (LTSP)	118.9
NTSP(Adj)	117.3

GEH Setpoint Calculation Methodology Without an AL

In the case where there is no AL, such as for the APRM Flow Biased STP Scram setpoint function, then the input to the setpoint calculation is an AV, instead of an AL. For such a case, NTSP1, the LTSP is not pertinent and cannot be calculated.

When the input to the setpoint calculation is the AV, then margin is calculated by GEH methodology between the AV and the NTSP (Adj), as discussed above.

PRNM Channel Performance Data

The PRNM uses an analog front end to interface with the Recirculation Loops flow sensors and the LPRM sensors. Processed data from this analog front end is converted to digital data using 16 bit analog to digital (A/D) conversion. For the electronic signal processing errors used in the setpoint calculations, only the errors (accuracy and drift) of the PRNM analog front end (and associated sample and hold circuit and A/D conversion) are pertinent. There is no error associated with the downstream digital signal processing because that is done by firmware algorithms. The trip function is also performed digitally, so that has no error, and a trip setting in firmware will not drift from one calibration to the next. Therefore, there is no setting tolerance (such as an As-Left Tolerance) for the PRNM digital trip setting.

For the PRNM fixed APRM Neutron Flux High setpoint and APRM Setdown setpoint functions, the instrument error is from components that can be calibrated within the PRNM APRM electronics. These PRNM errors are due to the accuracy and drift of the analog LPRM processing modules in the front end which process the LPRM detector signals, and their associated A/D conversion. The errors for each LPRM processor are specified conservatively in the PRNM specifications, and these independent random errors are combined statistically to determine the overall APRM electronics error.

For the flow biased APRM STP high setpoint functions, additional errors are considered, including errors due to accuracy, drift, and calibration of the Recirculation Loop flow transmitters (FTs), and errors due to the accuracy and drift of the analog flow processing modules in the PRNM front end that are used to process the flow signals.

The GEH PRNM LTR (page H-7 of Reference 1(c)) defines that the Channel Calibration is the calibration test performed at the stated calibration interval (typically the refueling interval), which (based on PRNM procedures) corresponds to the calibration performed by the "Auto-Calibration" process. This channel calibration surveillance procedure corresponds to Surveillance Requirement (SR) 3.3.1.1.10 at CGS. In this test each of the front end analog amplifiers (for neutron flux and flow monitoring) are calibrated using an internal calibration circuit, and the internal calibration circuit components (resistors and voltages) are calibrated using an external calibration source, and reset to the normal "un-drifted" state after calibration. In addition to assuring the devices are reset to their normal "un-drifted" state after calibration, a measurement of the drift of the devices before calibration is required to assure that the devices have satisfactory performance.

The APRM and its components are calibrated by several different surveillance tests in the TS. Each APRM channel is calibrated every 7 days as a system in CGS SR 3.3.1.1.2 where the APRM gain is

adjusted so that the APRM output matches the heat balance to within a prescribed amount (i.e., 2%). The gain adjustment compensates for changes in all parts of the system and is the appropriate test basis for calculating the AV and setpoints (NTSP1 and the final adjusted $NTSP_F$) for the APRM setpoint functions. The pertinent errors for this SR are used to calculate APRM setpoints by GEH methodology for both the new digital PRNM and the older analog APRM equipment that the PRNM replaced. For PRNM, the APRM trip setpoint is set in firmware and does not drift once it is set. The individual components of the PRNM APRM system that could drift and are calibrated are the analog components at the front end of the PRNM that process the inputs from the LPRM detectors and flow transmitters. The PRNM front end is tested and calibrated by CGS SR 3.3.1.1.10 including the Recirculation flow transmitters, where applicable. [This document will not discuss the performance of the Recirculation flow transmitters, including when discussing SR 3.3.1.1.10.]

For CGS SR 3.3.1.1.10, all the analog components in the PRNM that could drift are calibrated, so that after calibration the entire PRNM chassis is calibrated to perform according to its design and performance specifications for the next operating cycle. In this SR 3.3.1.1.10 calibration, the analog front end of the PRNM equipment is calibrated once every 24 months and the LPRM detectors are excluded. The LPRM detectors are calibrated as devices according to CGS SR 3.3.1.1.7. The SR 3.3.1.1.10 calibration is performed by the PRNM "Auto-Calibration" procedure which involves sending a known calibrated current into each LPRM and flow amplifier and internally adjusting the output after it is processed by the amplifier, and the associated sample-and-hold and A/D converter circuits, for any drift that may have occurred since the previous calibration.

A simple way of determining drift since the last "Auto-Calibration" is to run the PRNM "Cal Check" procedure on each LPRM or flow amplifier, just before running the "Auto-Calibration" procedure to bring the devices back into calibration. When "Cal Check" is performed on a selected PRNM LPRM or flow amplifier, the embedded software (firmware) in the PRNM internally disconnects the actual LPRM detector or flow transmitter input to the selected amplifier and connects the amplifier input to a precision current source designed to give a specified output if the amplifier has not drifted and is at its desired value. If the amplifier has drifted since the last "Auto-Calibration", the amount it has drifted can be determined by plant personnel from the outputs displayed on the PRNM/APRM screen. No manual calibration equipment is required when this "Cal Check" process is used. The "Cal Check" procedure provides the as-found values (AFVs) for a user selected calibration point for each PRNM LPRM and flow amplifier. "Cal Check" returns the measured AFV which can be manually subtracted from the user selected value to determine how much the device has drifted. This measured drift is also referred to as the AFV and is in units of % LPRM power for LPRM amplifiers and % loop flow for the flow amplifiers. Plant personnel can record the measured AFVs for later comparisons to determine if the device has performed as expected or whether it has degraded. Assuming this method is used for the AFVs, the "Cal Check" procedure would need to be included as part of CGS SR 3.3.1.1.10 calibration procedures.

When "Auto-Calibration" is performed, the gain and offset of each amplifier are adjusted automatically by the PRNM firmware to compensate for instrument drift and provide the correct output. This automatically assures that the as-left values (ALVs) after "Auto-Calibration" are within the predetermined calibration procedure ALTs. Assuming this method is used for the ALVs, the

"Auto-Calibration" procedure would need to be included as part of SR 3.3.1.1.10 calibration procedures.

Assuming the AFVs are acceptable, the "Auto-Calibration" procedure automatically returns each analog front end processor to the desired state after calibration. No manual adjustments are required. However, if the AFVs are not indicating acceptable instrument performance, then additional instrument evaluations may need to be performed. If necessary the device may need to be repaired or replaced before the "Auto-Calibration" procedure is performed to bring the devices into calibration. Because "Auto-Calibration" automatically returns all devices to their normal "undrifted" state, no subsequent manual actions are necessary. If confirmation of the as left condition is required, the "Cal Check" procedure can be run again immediately after "Auto Calibration" to assure that the devices have been reset to within their ALTs.

Note that the pertinent portions of the CGS SR 3.3.1.1.10 calibration procedures test and calibrate all the analog LPRM neutron flux and Recirculation Flow signal processing devices at the front end of the PRNM, because these devices can drift. It does not test the portion of the PRNM that performs the downstream processing of these signals in firmware. Thus, the SR does not test the APRM signal processing portion of the PRNM (which averages the signals from the various LPRM amplifiers) or the APRM flow processing (which adds the flow signals from the two Recirculation Flow loops), nor does it test the processing that generates the APRM trip signal because this processing is done in PRNM firmware and is not subject to drift. So the calibration tolerances for any surveillance of this portion of the PRNM signal processing and trip signal generation are zero.

Setpoint Calculation - Non-OPRM - CGS Specific

APRM setpoint calculations were performed to support installation of PRNMS at CGS. The APRM Flow Biased STP-High setpoint was calculated to support PRNM and ARTS/MELLLA. Calculations included scrams and rod blocks. All calculations were based on the error terms associated with the upgraded PRNMS equipment. ALTs (the tolerance within which the device calibration reading is left after calibration) were considered in the calculations; these tolerances were based on the existing Recirculation Loop flow transmitters, and PRNMS flow and power electronics. The AV/NTSP margin includes instrument loop accuracy under calibration conditions, instrument calibration errors, and instrument drift errors. [[

]]

For the APRM Flow Biased STP setpoint functions, some of the instrument errors are related to the Flow instruments used to measure Recirculation Drive (Loop) flows. Flow errors were converted to Power errors using the slope of the power-flow AVs, such that all errors were combined using the same unit of Percent RTP (% RTP).

Table 9.3.8-2 summarizes the limits, ALs or AVs, associated with the PRNMS setpoint calculations for CGS. Columns for both CLTP and PRNMS (ARTS/MELLLA) values are shown. If a setpoint is not credited in a SE, there is no applicable AL, per GEH setpoint methodology.

Table 9.3.8-2 PRNMS Setpoint Calculations for CGS

Setpoint Function	CLTP (% RTP)	PRNMS (ARTS/MELLLA) (% RTP)	Source / Basis
APRM Flow Biased STP Scram † **AVs**	TLO: 0.58 Wd + 62 SLO: 0.58 Wd + 62	TLO: 0.63 Wd + 64.0 SLO: 0.63 Wd + 60.8	Protects against slow reactivity transients (Reference 85)
APRM Flow Biased STP Rod Block † **AVs**	TLO: 0.58 Wd + 53 SLO: 0.58 Wd + 53 (Same as TLO)	TLO: 0.63 Wd + 60.1 SLO: 0.63 Wd + 56.9	Prevents rod withdrawal and alerts the Operator if the power is significantly above licensed power level; the rod block function precedes a flow-biased Scram (Reference 85)
APRM STP Scram Clamp † **AV**	114.9	114.9	Protects against slow reactivity transients. (Reference 85)
APRM Rod Block Clamp † **AV**	None	111	Prevents rod withdrawal and alerts the Operator if the power is significantly above licensed power level; the rod block function precedes a Scram (Reference 85)

† An AL is not applicable because this setpoint function is not used in any safety or transient analyses.

Reference 100 provides representative calculation summaries and is available for NRC review.

Setpoints -- OPRM

The OPRM setpoints are the nominal setpoints, which are established using a comprehensive BWR Owners' Group (BWROG) methodology for stability analysis approved by the NRC (Reference 101). There is no AL or AV with defined instrument error margins to the NTSP for the OPRM setpoints. Note that OPRM setpoints are not considered to be Limiting Safety System Settings (LSSSs) because stability is a special event, and not an Anticipated Operational Occurrence (AOO) which define LSSSs.

The following OPRM setpoints will be in the Core Operating Limits Report (COLR).

- OPRM Upscale Oscillation Amplitude
- OPRM Upscale Successive Confirmation Count (SCC)

- OPRM Trip Enable, APRM STP
- OPRM Trip Enable, Recirculation Drive Flow
- OPRM Operable, Thermal Power

The OPRM Upscale function setpoints (Period Based Algorithm Oscillation Amplitude and SCC setpoints) are established as nominal values based on cycle specific reload stability analyses in accordance with Reference 101.

The OPRM Upscale function auto-enable (not bypassed) region is established generically to correspond to reactor power greater than or equal to 30% of rated, and core flow (implemented as Recirculation drive flow) less than or equal to 60% of rated per Reference 101. Note that it is conservative to use Recirculation drive flow in place of core flow for the OPRM Upscale function auto-enable region boundary. The OPRM Upscale function auto-enable region is confirmed by a cycle-specific analysis each reload, and expanded if necessary. The OPRM Operable Thermal Power setpoint is established as 5% of rated power less than the OPRM Trip Enable, APRM STP per Reference 1.

OPRM Upscale function auto-enable (not bypassed) power and core flow setpoints are permissive setpoints. These setpoints are not explicitly modeled in stability analyses. Because permissives or interlocks are only one of multiple conservative starting assumptions for the accident analysis, they are generally considered as nominal values without regard to measurement accuracy.

Use of nominal setpoints for the OPRM Upscale function has been addressed during the licensing of the PRNMS at Browns Ferry Unit 1 (Reference 102) and at Monticello (Reference 103) previously. Note also that the OPRM trip setpoints are not listed in the BWR/4 Standard TS (STS, Reference 3).

Demonstration calculations for the nominal setpoints of the OPRM Upscale function are available for review. The associated analyses may be viewed by the NRC at a GEH office, upon request, and to a schedule agreed to by GEH and the NRC.

9.4 IEEE 603, Clause 7, Execute Features

Requirement: *In addition to the functional and design requirements in Section 5, the following requirements shall apply to the execute features:*

Per Section 2 of IEEE Standard 603-1991 (Reference 71), "execute features" are defined as, "the electrical and mechanical equipment and interconnections that perform a function, associated directly or indirectly with a safety function, upon receipt of a signal from the sense and command features. The scope of the execute features extends from the sense and command features output to and including the actuated equipment-to-process coupling."

The PRNM system upgrade generally replaces only the sense and command features. The execute features for RPS are considered to be the RPS trip actuators and pilot scram valve solenoids. For conservatism, the output relays from the PRNM system will also be considered as part of the execute features for the purposes of this evaluation.

9.4.1 IEEE 603, Clause 7.1, Automatic Control

Requirement: *Capability shall be incorporated in the execute features to receive and act upon automatic control signals from the sense and command features consistent with 4.4 of the design basis.*

Clause 4.4 of IEEE Standard 603-1991 (Reference 71) requires that the variables or combination of variables, or both, that are to be monitored to manually or automatically, or both, control each protective action; the analytical limit associated with each variable, the ranges (normal, abnormal, and accident conditions); and the rates of changes of these variables to be accommodated until proper completion of the protective action is ensured.

The protective action provided by the PRNM system is a reactor trip, via the RPS. The output relays of the PRNMS are the only execute features affected from the PRNM system upgrade. Per Section 2.1.2 of Reference 1(a), fiber-optic isolated solid state relays replace electro-mechanical output relays used in the current system. A 2-Out-Of-4 voter channel is added between the APRM channel and the existing RPS logic, but does not change the actual RPS interface or trip logic. Per Section 4.4.1.1.1 of Reference 1(a), the voter channels provide redundant outputs, each one driving a separate interface relay (unchanged from the current RPS interface). Thus, the output of the voter channels replicates the original APRM interface. Per Section 1.4.12, the original time response requirements of the system are retained and satisfied by the PRNM system.

One deviation from Reference 1(a) is taken for the CGS PRNM system. For the CGS PRNM, the OPRM Upscale function is combined with the APRM Inop function as the OPRM channel input to be voted. This deviation is fully explained and justified within Enclosure 1 of Reference 14.

As stated in Section 4.4.1.1.16 of Reference 1(a), completion of protective action, once initiated, is accomplished by the RPS. The only protective action is therefore the trip output when required.

As demonstrated in the above discussion, the capability has been incorporated in the execute features to receive and act upon automatic control signals from the sense and command features consistent with the design basis, which is unchanged from the original analysis for the PRM system.

9.4.2 IEEE 603, Clause 7.2, Manual Control

Requirement: *If manual control of any actuated component in the execute features is provided, the additional design features in the execute features necessary to accomplish such manual control shall not defeat the requirements of 5.1 and 6.2. Capability (of manual control) shall be provided in the execute features to receive and act upon manual control signals from the sense and command features consistent with the design basis.*

For the PRNM system, there are no manually controlled actions for which no automatic control is provided that are required for the safety systems to accomplish their safety functions. Thus, this requirement does not apply to the PRNM system upgrade.

9.4.3 IEEE 603, Clause 7.3, Completion of Protective Action

Requirement: *The design of the execute features shall be such that once initiated, the protective actions of the execute features shall go to completion. This requirement shall not preclude the use of equipment protective devices identified in 4.11 of the design basis or the provision for deliberate operator interventions. When the sense and command features reset, the execute features shall not automatically return to normal; they shall require separate, deliberate operator action to be returned to normal. After the initial protective action has gone to completion, the execute features may require manual control or automatic control (that is, cycling) of specific equipment to maintain completion of the safety function.*

As stated in Section 4.4.1.1.16 of Reference 1(a), completion of a protective action (RPS trip), once initiated, is accomplished by the RPS, as it is currently designed. Per Section 3.15 of the SER (Reference 2), the PRNM system provides trip signals to the RPS. Because the RPS trip system is not being modified as part of the PRNM system, once tripped, the RPS reactor trip will proceed to completion as currently designed.

The NRC staff evaluated and approved the PRNM system design with regard to completion of protective action once it is initiated in Section 3.15 of the SER (Reference 2), based on the PRNM system compliance with IEEE Standard 279-1971 (Reference 86) requirement criteria (paragraph 4.16), as described in Section 4.4.1.1.16 of the LTR (Reference 1(a)).

9.4.4 IEEE 603, Clause 7.4, Operating Bypass

Requirement: *Whenever the applicable permissive conditions are not met, a safety system shall automatically prevent the activation of an operating bypass or initiate the appropriate safety function(s). If plant conditions change so that an activated operating bypass is no longer permissible, the safety system shall automatically accomplish one of the following actions:*

(1) Remove the appropriate active operating bypass(es).

(2) Restore plant conditions so that permissive conditions once again exist.

(3) Initiate the appropriate safety function(s).

As stated in Section 4.4.1.1.12 of Reference 1(a), the original analysis for the PRM applies for the APRM and OPRM trip functions in the PRNM, with respect to operating bypasses. There are no automatic bypasses for the APRM trip function. The OPRM includes "enabling logic" that automatically activates the trip output only in certain operating zones in the power/flow map (nominally above 30% power and below 60% flow). The APRM trip setpoint is automatically changed to a lower value (setdown) when the manually operated reactor mode switch is not in RUN.

The NRC staff evaluated and approved the PRNM system design with regard to operating bypasses in Section 3.11 of the SER (Reference 2). NRC approval of the design was based on PRNM system compliance with Reference 86 requirement criteria (paragraph 4.12), as described in Sections 4.4 and 5.3 of the LTR (Reference 1(a)).

9.4.5 IEEE 603, Clause 7.5, Maintenance Bypass

Requirement: *The capability of a safety system to accomplish its safety function shall be retained while execute features equipment is in maintenance bypass. Portions of the execute features with a degree of redundancy of one shall be designed such that when a portion is placed in maintenance bypass (that is, reducing temporarily its degree of redundancy to zero), the remaining portions provide acceptable reliability.*

As stated in Section 9.4, the PRNM system upgrade generally replaces only the sense and command features. The execute features for RPS are considered to be the RPS trip actuators and pilot scram valve solenoids. For conservatism, the output relays from the PRNM system will also be considered as part of the execute features for the purposes of this evaluation.

Per Section 2.1.2 of Reference 1(a), fiber-optic isolated solid state relays replace electro-mechanical output relays used in the current system. A 2-Out-Of-4 voter channel is added between the APRM channel and the existing RPS logic, but does not change the actual RPS interface or trip logic. Per Section 4.4.1.1.1 of Reference 1(a), the voter channels provide redundant outputs, each one driving a separate interface relay (unchanged from the current RPS interface).

The PRNM system is designed to allow one APRM/OPRM channel, but no voter channels, to be bypassed. A trip from any one unbypassed APRM or OPRM function will result in a "half-trip" in all four of the voter channels, but no trip inputs to either RPS trip system. A trip from any two unbypassed APRM or OPRM channels will result in a full trip in each of the four voter channels, which in turn results in two trip inputs into each RPS trip system. Three of the four APRM / OPRM channels and all four of the voter channels are required to be operable to ensure that no single instrument failure will preclude a scram from this function on a valid signal.

Therefore, the execute features modified by the PRNM system upgrade are not allowed to be in maintenance bypass, and Clause 7.5 of IEEE Standard 603-1991 (Reference 71) does not apply to this upgrade.

9.5 IEEE 603, Clause 8, Power Source Requirements

9.5.1 IEEE Standard 603, Clause 8.1, Electrical Power Sources

Requirement: *Those portions of the Class 1E power system that are required to provide the power to the many facets of the safety system are governed by the criteria of this document and are a portion of the safety systems. Specific criteria unique to the Class 1E power systems are given in IEEE Standard 308-1980.*

This criterion is not applicable to the CGS PRNM system design.

9.5.2 IEEE Standard 603, Clause 8.2, Non-Electrical Power Sources

Requirement: *Non-electrical power sources, such as control-air systems, bottled-gas systems, and hydraulic systems, required to provide the power to the safety systems are a portion of the safety systems and shall provide power consistent with the requirements of this standard.*

Specific criteria unique to non-electrical power sources are outside the scope of this standard and can be found in other standards.

The PRNM system does not require any non-electrical power sources; therefore, this criterion is not applicable to the CGS PRNM system design or the systems supplying power to the PRNM system.

9.5.3 IEEE Standard 603, Clause 8.3, Maintenance Bypass

Requirement: *The capability of the safety systems to accomplish their safety functions shall be retained while power sources are in maintenance bypass. Portions of the power sources with a degree of redundancy of one shall be designed such that when a portion is placed in maintenance bypass (that is, reducing temporarily its degree of redundancy to zero), the remaining portions provide acceptable reliability.*

This criterion is not applicable to the CGS PRNM system design.

10. Conformance with IEEE Standard 7-4.3.2

This License Amendment Request includes ARTS/MELLLA changes, as well as a digital upgrade for the PRNM system. The changes for ARTS/MELLLA implementation are justified within NEDC-33507P (Reference 85), and are considered separately from the PRNM system digital upgrade. IEEE Standard 7-4.3.2 only applies to the digital upgrade; therefore, the ARTS/MELLLA changes are not addressed in the following sub-sections.

10.1 Regulatory Evaluation

For nuclear plants with construction permits issued before January 1, 1971, 10 CFR 50.55a(h) requires that protection systems must be consistent with their licensing basis or may meet the requirements of IEEE Standard 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995. For nuclear power plants with construction permits issued after January 1, 1971, but before May 13, 1999, 10 CFR 50.55a(h) requires that protection systems must meet the requirements stated in either IEEE Standard 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations," or IEEE Standard 603-1991 and the correction sheet dated January 30, 1995. Applications filed on or after May 13, 1999 for construction permits and operating licenses, must meet the requirements for safety systems in IEEE Standard 603-1991 and the correction sheet dated January 30, 1995.

IEEE Standard 603-1991 does not directly discuss digital systems, but states that guidance on the application of the criteria in IEEE Standard 603-1991 for safety systems using digital programmable computers is provided in IEEE/ANS Standard 7-4.3.2-1982, "American Nuclear Society and IEEE Standard Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations." IEEE/ANS Standard 7-4.3.2-1982 has been revised into IEEE Standard 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations." Guidance on applying the safety system criteria to computer based safety systems is provided by IEEE Standard 7-4.3.2-2003, as endorsed by Regulatory Guide 1.152, Revision 2, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants." IEEE Standard 7-4.3.2-2003 specifies computer-specific criteria (incorporating hardware, software, firmware, and interfaces) to supplement the criteria in IEEE Standard 603-1998. Although IEEE Standard 7-4.3.2-2003 references IEEE Standard 603-1998, IEEE Standard 603-1991 and the correction sheet dated January 30, 1995 remains the requirement for safety systems in accordance with 10 CFR 50.55a(h). SRP Appendix 7.1-D contains guidance for the evaluation of conformance to IEEE Standard 7-4.3.2-2003.

While IEEE Standard 7-4.3.2 is not codified in 10CFR50.55a, it is the principal standard used by the NRC staff in evaluating digital I&C upgrades. This standard is endorsed by RG 1.152 Revision 2 dated 2003 (i.e., RG 1.152 & IEEE Standard 7-4.3.2 are SRP acceptance criteria). To demonstrate conformance with another standard in lieu of IEEE Standard 7-4.3.2, the licensee should include an evaluation that allows the NRC staff to conclude that conformance provides a high quality system. This activity should be expected to take a significant amount of additional review time and effort.

10.2 IEEE Standard 7-4.3.2, Clause 4, Safety System Design Basis

Requirement: *No requirements beyond IEEE Standard 603-1998 are necessary.*

Per DI&C-ISG-06 (Reference 15), Section D.10.4.1, "Clause 4 does not provide any additional criteria beyond those in IEEE Standard 603-1991. Therefore, this clause should be addressed by the review performed under Section D.9.4.1." No further analysis is required in this section.

10.3 IEEE Standard 7-4.3.2, Clause 5, System

Requirement: *The following subclauses list the safety system criteria in the order they are listed in IEEE Standard 603-1998. For some criteria, there are no additional requirements beyond what is stated in IEEE Standard 603-1998. For other criteria, additional requirements are described in 5.1 through 5.15.*

Per DI&C-ISG-06 (Reference 15), Section D.10.4.2, "Clause 5 contains no additional criteria beyond those in IEEE Standard 603-1991; however, some of the sub-clauses contain additional criteria. The sub-clauses are described in 5.1 through 5.15." No further analysis is required in this section.

10.3.1 IEEE Standard 7-4.3.2, Clause 5.1, Single-Failure Criterion

Requirement: *No requirements beyond IEEE Standard 603-1998 are necessary.*

Per DI&C-ISG-06 (Reference 15), Section D.10.4.2.1, "There are no criteria beyond those in IEEE Standard 603-1991. Therefore, this clause should be addressed by the review performed under Section D.9.4.2.1." No further analysis is required in this section.

10.3.2 IEEE Standard 7-4.3.2, Clause 5.2, Completion of Protective Actions

Requirement: *No requirements beyond IEEE Standard 603-1998 are necessary.*

Per DI&C-ISG-06 (Reference 15), Section D.10.4.2.2, "There are no criteria beyond those in IEEE Standard 603-1991. Therefore, this clause should be addressed by the review performed under Section D.9.4.2.2." no further analysis is required in this section.

10.3.3 IEEE Standard 7-4.3.2, Clause 5.3, Quality

Requirement: *Hardware quality is addressed in IEEE Standard 603-1998. Software quality is addressed in IEEE/EIA Standard 12207.0-1996 and supporting standards. Computer development activities shall include the development of computer hardware and software. The integration of the computer hardware and software and the integration of the computer with the safety system shall be addressed in the development process.*

A typical computer system development process consists of the following life cycle processes:

— *Creating the conceptual design of the system, translation of the concepts into specific system requirements*

— *Using the requirements to develop a detailed system design*

— *Implementing the design into hardware and software functions*

— *Testing the functions to assure the requirements have been correctly implemented*

— *Installing the system and performing site acceptance testing*

— *Operating and maintaining the system*

— *Retiring the system*

In addition to the requirements of IEEE Standard 603-1998, the following activities necessitate additional requirements that are necessary to meet the quality criterion:

— *Software development*

— *Qualification of existing commercial computers (see 5.4.2)*

— *Use of software tools*

— *V&V*

— *Configuration management*

— *Risk Management*

Section 4.4 (Software Development Process) describes in detail the life cycle processes applicable to the CGS PRNMS programmable entities. Summarizing briefly, GEH adhered to the same NUMAC software development and testing process used for previous NUMAC PRNM projects. That process had been evaluated and approved based on earlier revisions of NRC Regulatory Guidance and standards (see Appendix A of Reference 1(b) and Section 3.2 of Reference 2). As discussed in Section 4.4.8, CGS PRNMS Software V&V Process & IEEE 1012-1998 (Reference 35) Requirements, [[

]]

At the conclusion of these efforts, the CGS PRNM will have been developed using a life cycle process that aligns well with the life cycle process defined by IEEE Standard 1012-1998 (Reference 35).

10.3.3.1 IEEE Standard 7-4.3.2, Clause 5.3.1, Software Development

Requirement: *Computer software shall be developed, modified, or accepted in accordance with an approved software quality assurance (QA) plan consistent with the requirements of IEEE/EIA 12207.0-1996. The software QA plan shall address all software that is resident on the computer*

at run time (i.e., application software, network software, interfaces, operating systems, and diagnostics). Guidance for developing software QA plans can be found in IEC 60880 (1986-09) and IEEE Standard 730™-1998.

GEH developed the CGS PRNM, including the software, under the GEH QA program. A discussion of this program, with reference to DI&C ISG-06 (Reference 15) D.4.4.1.3, SQAP, is provided in Section 4.4.1.3 (Software Quality Assurance Plan). The tools that were used during development and testing are described in Section 4.4.6 (Development and Production Tools).

10.3.3.1.1 IEEE Standard 7-4.3.2, Clause 5.3.1.1, Software Quality Metrics

The use of software quality metrics shall be considered throughout the software life cycle to assess whether software quality requirements are being met. When software quality metrics are used, the following lifecycle phase characteristics should be considered:

- *— Correctness/Completeness (Requirements phase)*
- *— Compliance with requirements (Design phase)*
- *— Compliance with design (Implementation phase)*
- *— Functional compliance with requirements (Test and Integration phase)*
- *— On-site functional compliance with requirements (Installation and Checkout phase)*
- *— Performance history (Operation and Maintenance phase)*

The basis for the metrics selected to evaluate software quality characteristics should be included in the software development documentation. IEEE Standard 1061™-1998 provides a methodology for the application of software quality metrics.

The GEH NUMAC process does not specify software quality metrics. However, the Baseline Review process is used throughout the software development life cycle to ensure that software requirements are being met, as discussed in Section 4.4.1.10 (SVVP) and Section 4.4.5.1 (Microprocessor Firmware Development). GEH also used a thorough testing program to evaluate the software and the integrated system, as discussed in Sections 4.4.1.12 (Software Test Plan), 4.4.2.4 (Testing Activities), and 2.4.13 (Testing). The layered testing approach included evaluations of the software in the development environment, as well as evaluations of the integrated system, which included the embedded firmware installed on the actual target equipment. The test results were documented and defects were addressed.

10.3.3.2 IEEE Standard 7-4.3.2, Clause 5.3.2, Software Tools

Requirement: *Software tools used to support software development processes and verification and validation (V&V) processes shall be controlled under configuration management.*

One or both of the following methods shall be used to confirm the software tools are suitable for use:

- *a) A test tool validation program shall be developed to provide confidence that the necessary features of the software tool function as required.*

b) The software tool shall be used in a manner such that defects not detected by the software tool will be detected by V&V activities.

Tool operating experience may be used to provide additional confidence in the suitability of a tool, particularly when evaluating the potential for undetected defects.

The software tools used to support software development processes and V&V processes are controlled under the NUMAC software configuration management plan. The software tools are used in a manner such that defects not detected by the software tools are detected by V&V activities. Section 4.4.1.2, Software Development Processes, provides a description of the processes used. The NUMAC design approach is in accordance with the criterion from IEEE Standard 7-4.3.2 2003 (Reference 45), Clause 5.3.2, "Software Tools," as endorsed by RG 1.152 (Reference 46). Section 4.4.1.10, SVVP, describes the specific V&V activities. Section 4.4.6, Development and Production Tools, addresses the use of software tools in detail. Additional information on software tools is provided in Section 4.4.3.5, System Build Documents, Section 4.4.5.3.6.1, Scope/Coverage of V&V, and Section 4.4.6.1, Legacy PLD Firmware Development. Section 4.4.8 provides a detailed mapping of the approach that was in place during the PRNMS project to IEEE Standard 1012-1998 (Reference 35). [[

]]

A description of the Software Configuration Management Plan (SCMP) is provided in Section 4.4.1.11, Software Configuration Management Plan. The NUMAC SCMP in conjunction with standard GEH procedures establishes a software configuration management program for NUMAC products that is consistent with guidance provided in IEEE Standard 1074-1995 (Reference 43), Clause 7.2.4, "Plan Configuration Management," as endorsed by RG 1.173 (Reference 44) as well as guidance provided in IEEE Standard 828-1990 (Reference 58), as endorsed by RG 1.169 (Reference 59). The NUMAC SCMP used in conjunction with GEH procedures is also consistent with guidance provided in IEEE Standard 7-4.3.2-2003 (Reference 45) Clause 5.3.5, "Software configuration management." The NUMAC SCMP used in conjunction with standard GEH procedures provides for comparable configuration management of NUMAC software that is consistent with the objectives stated in the regulatory guidance, even though the NUMAC SCMP does not conform to the conventional model of a Software Configuration Management Plan as described in References 53 and 58. Additional configuration management activities are described in Section 4.4.2.3, Configuration Management Activities.

10.3.3.3 IEEE Standard 7-4.3.2, Clause 5.3.3, Verification and Validation

Requirement: *NOTE—See IEEE Standard 1012-1998 and IEEE Standard 1012a™-1998 for more information about software V&V.*

V&V is an extension of the program management and systems engineering team activities. V&V is used to identify objective data and conclusions (i.e., proactive feedback) about digital system quality, performance, and development process compliance throughout the system life cycle. Feedback consists of anomaly reports, performance improvements, and quality improvements

regarding the expected operating condition across the full spectrum of the system and its interfaces.

V&V processes are used to determine whether the development products of an activity conform to the requirements of that activity, and whether the system performs according to its intended use and user needs. This determination of suitability includes assessment, analysis, e valuation, review, inspection, and testing of products and processes.

This standard adopts the IEEE Standard 1012-1998 terminology of process, activity and task, in which software V&V processes are subdivided into activities, which are further subdivided into tasks. The term V&V effort is used to reference this framework of V&V processes, activities, and tasks.

V&V processes shall address the computer hardware and software, integration of the digital system components, and the interaction of the resulting computer system with the nuclear power plant.

The V&V activities and tasks shall include system testing of the final integrated hardware, software, firmware, and interfaces.

The software V&V effort shall be performed in accordance with IEEE Standard 1012-1998. The IEEE Standard 1012-1998 V&V requirements for the highest integrity level (level 4) apply to systems developed using this standard (i.e., IEEE Standard 7-4.3.2™). See IEEE Standard 1012-1998 Annex B for a definition of integrity level 4 software.

The V&V program included [[

]]

The V&V process provides an objective assessment of the software products and processes throughout the lifecycle, addresses both hardware and software, integration of the entire system, and interaction with plant systems.

10.3.3.4 IEEE Standard 7-4.3.2, Clause 5.3.4, Independent V&V

Requirement: *The previous section addresses the V&V activities to be performed. This section defines the levels of independence required for the V&V effort. IV&V activities are defined by three parameters: technical independence, managerial independence, and financial independence. These parameters are described in Annex C of IEEE Standard 1012-1998.*

The development activities and tests shall be verified and validated by individuals or groups with appropriate technical competence, other than those who developed the original design.

Oversight of the IV&V effort shall be vested in an organization separate from the development and program management organizations. The V&V effort shall independently select

a) The segments of the software and system to be analyzed and tested,

b) The V&V techniques, and

c) The technical issues and problems upon which to act.

The V&V effort shall be allocated resources that are independent of the development resources.

See Annex C of IEEE Standard 1012-1998 for additional guidance.

Section 4.4.8 (CGS PRNMS Software V&V Process & IEEE 1012-1998 Requirements), provides [[

]] oversight of the IV&V effort will be vested in the Chief Engineers Office, an organization that is separate from the development and program management organizations.

10.3.3.5 IEEE Standard 7-4.3.2, Clause 5.3.5, Software Configuration Management

Requirement: *Software configuration management shall be performed in accordance with IEEE Standard 1042-1987. IEEE Standard 828™-1998 provides guidance for the development of software configuration management plans.*

The minimum set of activities shall address the following:

a) Identification and control of all software designs and code

b) Identification and control of all software design functional data (e.g., data templates and data bases)

c) Identification and control of all software design interfaces

d) Control of all software design changes

e) Control of software documentation (user, operating, and maintenance documentation)

f) Control of software vendor development activities for the supplied safety system software

g) Control and retrieval of qualification information associated with software designs and code

h) Software configuration audits

i) Status accounting

Some of these functions or documents may be performed or controlled by other QA activities. In this case, the software configuration management plan shall describe the division of responsibility.

A software baseline shall be established at appropriate points in the software life cycle process to synchronize engineering and documentation activities. Approved changes that are created subsequent to a baseline shall be added to the baseline.

The labeling of the software for configuration control shall include unique identification of each configuration item, and revision and/or date time stamps for each configuration item.

Changes to the software/firmware shall be formally documented and approved consistent with the software configuration management plan. The documentation shall include the reason for the change, identification of the affected software/firmware, and the impact of the change on the system. Additionally, the documentation should include the plan for implementing the change in

the system (e.g., immediately implementing the change, or scheduling the change for a future version).

Section 4.4.1.11 (Software Configuration Management Plan) provides a description of the NUMAC SCMP and how it is used in conjunction with GEH procedures in order to establish a software configuration management program for NUMAC products.

Summarizing briefly, the process makes use of existing GEH procedures that govern configuration control in a general way in order to provide control of the particular documents that are defined for software. A series of Baseline Reviews provide oversight and assurance that the process was followed throughout the project. Section 4.4.2.3 (Configuration Management Activities) provides a discussion of the activities undertaken during the project, in order comply with the SCMP. Section 4.4.7 (Development & Programming of Microprocessor & PLD Firmware – Identification) describes the method for labeling the released firmware and PLD components.

10.3.3.6 IEEE Standard 7-4.3.2, Clause 5.3.6, Software Project Risk Management

Requirement: *Software project risk management is a tool for problem prevention: identifying potential problems, assessing their impact, and determining which potential problems must be addressed to assure that software quality goals are achieved. Risk management shall be performed at all levels of the digital system project to provide adequate coverage for each potential problem area. Software project risks may include technical, schedule, or resource-related risks that could compromise software quality goals, and thereby affect the ability of the safety computer system to perform safety related functions. Software project risk management differs from hazard analysis, as defined in 3.1.31, in that hazard analysis is focused solely on the technical aspects of system failure mechanisms.*

Risk management shall include the following steps:

a) Determine the scope of risk management to be performed for the digital system.

b) Define and implement appropriate risk management strategies.

c) Identify risks to the software project in the project risk management strategy and as they develop during the conduct of the project.

d) Analyze risks to determine the priority for their mitigation.

e) Develop risk mitigation plans for risks that have the potential to significantly impact software quality goals, with appropriate metrics for tracking resolution progress. (These risks may include technical, schedule, or resource-related project risks that could compromise the ability of the safety computer system to perform safety related functions.)

f) Take corrective actions when expected quality is not achieved.

g) Establish a project environment that supports effective communications between individuals and groups for the resolution of software project risks.

Additional guidance on the topic of risk management is provided in IEEE/EIA 12207.0-1996, and IEEE Standard 1540-2001].

Project risk management is a key function of the CGS PWP. The PWP fully addresses the topics discussed in IEEE Standard 1074-1995 (Reference 43) Clause 3.1.6, "Plan Project Management," as endorsed by RG 1.173 (Reference 44) as well as IEEE Standard 7-4.3.2-2003 (Reference 45) Clause 5.3.6, "Software Project Risk Management," as endorsed by RG 1.152 Revision 2 (Reference 46). The PWP invokes GEH project risk management procedure P&P 10-29 (Reference 17). Section 4.4.1.1, SMP, provides a description of the CGS PWP.

Reference 17 provides the following instructions for the risk management applied for the CGS PRNM project. The appropriate risk management plan and implementation is determined at project inception. The PM and project team develops a plan for risk management, performs initial risk identification and analysis, and establishes the risk abatement plans. The PM monitors and controls risk response throughout the life of the project. The PM also monitors the project to identify and analyze new risks, and establish risk abatement plans in response to those risks. Though risks are considered at the beginning of a project, regular reviews are held throughout the life of the project to assess risks previously identified and to identify new risks.

[[

]]

In addition to the PWP and Reference 17, [[

]] Section 4.4.1.9, Software Safety Plan, provides a description of the Technical Reviews for the CGS PRNM.

In summary, the CGS PRNM project software project risk management activities are a tool for problem prevention: identifying potential problems, assessing their affect, and determining which potential problems are addressed to assure that software quality goals are achieved. Software project risks include technology, resources, schedule, and financial. Risk abatement identifies, evaluates, selects, and implements options to reduce risks to acceptable levels given project constraints and objectives. The PM monitors and controls risk response throughout the project life cycle using a method appropriate to the type, size, and scope of the project. The PM also monitors the project to identify and analyze new risks, and establish risk abatement plans in response to those risks. Risks are evaluated monthly in accordance with the type, size, and scope of the project.

10.3.4 IEEE Standard 7-4.3.2, Clause 5.4, Equipment Qualification

Requirement: *In addition to the equipment qualification criteria provided by IEEE Standard 603-1998, the requirements listed in 5.4.1 and 5.4.2 are necessary to qualify digital computers for use in safety systems.*

See the information below for responses to requirements listed in Reference 45, Clauses 5.4.1 and 5.4.2.

10.3.4.1 IEEE Standard 7-4.3.2, Clause 5.4.1, Computer System Testing

Requirement: *Computer system qualification testing (see 3.1.36) shall be performed with the computer functioning with software and diagnostics that are representative of those used in actual operation. All portions of the computer necessary to accomplish safety functions, or those portions whose operation or failure could impair safety functions, shall be exercised during testing. This includes, as appropriate, exercising and monitoring the memory, the CPU, inputs and outputs, display functions, diagnostics, associated components, communication paths, and interfaces. Testing shall demonstrate that the performance requirements related to safety functions have been met.*

The PRNM system equipment qualification testing and analysis specifically addresses performance of required safety functions during testing, using software and diagnostics that are representative of those used in actual operation. This specifically includes exercising the computer system equipment and monitoring of the appropriate system parameters during testing. See Section 5.

10.3.4.2 IEEE Standard 7-4.3.2, Clause 5.4.2, Qualification of Commercial Computers

Requirement: *NOTE—See Annex C for more information about commercial grade item dedication.*

The qualification process shall be accomplished by evaluating the hardware and software design using the criteria of this standard. Acceptance shall be based upon evidence that the digital system or component, including hardware, software, firmware, and interfaces, can perform its required functions. The acceptance and its basis shall be documented and maintained with the qualification documentation.

In those cases in which traditional qualification processes cannot be applied, an alternative approach to verify a component is acceptable for use in a safety-related application is commercial grade dedication. The objective of commercial grade dedication is to verify that the item being dedicated is equivalent in quality to equipment developed under a 10 CFR 50 Appendix B program [B16].

The dedication process for the computer shall entail identification of the physical, performance, and development process requirements necessary to provide adequate confidence that the proposed digital system or component can achieve the safety function. The dedication process shall apply to the computer hardware, software, and firmware that are required to accomplish the safety function. The dedication process for software and firmware shall, whenever possible, include an evaluation of the design process. There may be some instances in which a design process cannot be evaluated as part of the dedication process. For example, the organization performing the evaluation may not have access to the design process information for a microprocessor chip to be used in the safety system. In this case, it would not be possible to perform an evaluation to support the dedication. Because the dedication process involves all aspects of life cycle processes and manufacturing quality, commercial grade item dedication should be limited to items that are relatively simple in function relative to their intended use.

Commercial grade item dedication involves preliminary phase and detailed phase activities. These phase activities are described in 5.4.2.1 through 5.4.2.2.

Commercial grade software and commercial grade computer hardware are not used to perform any safety function in the NUMAC PRNM system. Therefore, the evaluation results provided in the LTR and this submittal indicate that the criteria of Clause 5.4.2 of Reference 45 are not applicable to the CGS PRNM system.

Note: The requirements in IEEE Standard 7-4.3.2, Subclauses 5.4.2.1 through 5.4.2.2 are not listed, since the overall Clause 5.4.2 has been determined not to apply to this system.

10.3.5 IEEE Standard 7-4.3.2, Clause 5.5, System Integrity

NEDC-33698P (Reference 88) evaluates the Power Range Neutron Monitoring System (PRNMS) upgrade, using the Acceptance Criteria identified in IEEE Standard 603-1991 (Reference 71), IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, Clause 5.5, System Integrity. Guidance on the application of this criteria for safety system equipment employing digital computers and software or firmware is found in IEEE Standard 7-4.3.2-2003 (Reference 45) Clause 5.5, Sub-clauses 5.5.1 (Design for Computer Integrity), 5.5.2 (Design for Test and Calibration) and 5.5.3 (Fault Detection and Self-diagnostics), and SRP Chapter 7, Appendix 7.1-D, Section 5.5. Compliance with the applicable requirements is shown primarily using the original LTR (Reference 1).

10.3.6 IEEE Standard 7-4.3.2, Clause 5.6, Independence

Requirement: *In addition to the requirements of IEEE Standard 603-1998, data communication between safety channels or between safety and non-safety systems shall not inhibit the performance of the safety function.*

IEEE Standard 603-1998 requires that safety functions be separated from non-safety functions such that the non-safety functions cannot prevent the safety system from performing its intended functions. In digital systems, safety and non-safety software may reside on the same computer and use the same computer resources.

Either of the following approaches is acceptable to address the previous issues:

a) Barrier requirements shall be identified to provide adequate confidence that the non-safety functions cannot interfere with performance of the safety functions of the software or firmware. The barriers shall be designed in accordance with the requirements of this standard. The non-safety software is not required to meet these requirements.

b) If barriers between the safety software and non-safety software are not implemented, the non-safety software functions shall be developed in accordance with the requirements of this standard.

Guidance for establishing communication independence is provided in Annex E.

Per DI&C-ISG-06 (Reference 44), Section D.10.4.2.6, Clause 5.6 specifies that in addition to the requirements of IEEE Standard 603-1991 (Reference 71), data communication between safety channels or between safety and non-safety systems not inhibit the performance of the safety function. The protection system should be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel that is common to both systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. The interconnection of the protection and control systems should be limited so as to assure that safety is not impaired.

DI&C-ISG-04 discussed communications independence, and if the licensee can demonstrate compliance with DI&C-ISG-04, this demonstration should also suffice for compliance with this clause. The licensee should point to documentation on compliance with DI&C-ISG-04."

Demonstration of compliance with IEEE Standard 7-4.3.2 (Reference 45), Clause 5.6 and DI&C-ISG-04 (Reference 13) is provided within NEDC-33697P (Reference 84).

10.3.7 IEEE Standard 7-4.3.2, Clause 5.7, Capability for Test and Calibration

NEDC-33698P (Reference 88) evaluates the PRNMS upgrade, using the Acceptance Criteria identified in IEEE Standard 603-1991 (Reference 71) Clause 5.7, Capability for Test and Calibration. IEEE Standard 7-4.3.2-2003 (Reference 45), Clause 5.7 contains no additional requirements or guidance beyond that identified in Reference 71.

10.3.8 IEEE Standard 7-4.3.2, Clause 5.8, Information Displays

Requirement: *No requirements beyond IEEE Standard 603-1998 are necessary.*

Per DI&C-ISG-06 (Reference 44), Section D.10.4.2.8, "Clause 5.8 states that there are no criteria beyond those found in IEEE Standard 603-1991; however, this is limited to equipment that has only a display function. Some displays may also include control functions, and therefore, need to

be evaluated to show that incorrect functioning of the information display does not prevent the performance of the safety function when necessary."

For the PRNM system, no control or protective actions are executed through the displays, and inadvertent actions, such as an unintended touch on a touch sensitive display cannot prevent the safety function. Therefore no further analysis is required in this section.

10.3.9 IEEE Standard 7-4.3.2, Clause 5.9, Control of Access

Requirement: *No requirements beyond IEEE Standard 603-1998 are necessary.*

Per DI&C-ISG-06 (Reference 15), Section D.10.4.2.9, "There are no criteria beyond those in IEEE Standard 603-1991. Therefore, this clause should be addressed by the review performed under Section D.9.4.2.9." No further analysis is required in this section.

10.3.10 IEEE Standard 7-4.3.2, Clause 5.10, Repair

NEDC-33698P (Reference 88) evaluates the PRNMS upgrade, using the Acceptance Criteria identified (Reference 71), Clause 5.10, Repair. Reference 45, Clause 5.10 contains no additional requirements or guidance beyond that identified in (Reference 71).

10.3.11 IEEE Standard 7-4.3.2, Clause 5.11, Identification

Requirement: *To provide assurance that the required computer system hardware and software are installed in the appropriate system configuration, the following identification requirements specific to software systems shall be met:*

a) Firmware and software identification shall be used to assure the correct software is installed in the correct hardware component.

b) Means shall be included in the software such that the identification may be retrieved from the firmware using software maintenance tools.

c) Physical identification requirements of the digital computer system hardware shall be in accordance with the identification requirements in IEEE Standard 603-1998.

Per DI&C-ISG-06 (Reference 15), Section D.10.4.2.11, "Clause 5.11 specifies that firmware and software identification be used to assure the correct software is installed in the correct hardware component. Means should be included in the software such that the identification may be retrieved from the firmware using software maintenance tools and that physical identification of hardware is implemented in accordance with IEEE Standard 603-1991 (Reference 71). The identification should be clear and unambiguous, include revision level, and should be traceable to configuration control documentation. Licensees should ensure that the configuration management plans are sufficient to meet this clause, and when discussing compliance with the clause, point to the sections of the configuration management plans where this is discussed. The NRC staff should review the development processes that were implemented and that the firmware and software identification is in accordance with NRC regulations."

Compliance with Clause 5.11 of IEEE Standard 7-4.3.2 (Reference 45) is fully discussed within Sections 4.4.7.

10.3.12 IEEE Standard 7-4.3.2, Clause 5.12, Auxiliary Features

Requirement: *No requirements beyond IEEE Standard 603-1998 are necessary.*

Per DI&C-ISG-06 (Reference 15), Section D.10.4.2.12, "There are no criteria beyond those in IEEE Standard 603-1991. Therefore, this clause should be addressed by the review performed under Section D.9.4.2.12." No further analysis is required in this section.

10.3.13 IEEE Standard 7-4.3.2, Clause 5.13, Multi-Unit Stations

Requirement: *No requirements beyond IEEE Standard 603-1998 are necessary.*

Per DI&C-ISG-06 (Reference 15), Section D.10.4.2.13, "There are no criteria beyond those in IEEE Standard 603-1991. Therefore, this clause should be addressed by the review performed under Section D.9.4.2.13." No further analysis is required in this section.

10.3.14 IEEE Standard 7-4.3.2, Clause 5.14, Human Factors Considerations

Requirement: *No requirements beyond IEEE Standard 603-1998 are necessary.*

Per DI&C-ISG-06 (Reference 15), Section D.10.4.2.14, "There are no criteria beyond those in IEEE Standard 603-1991. Therefore, this clause should be addressed by the review performed under Section D.9.4.2.14." No further analysis is required in this section.

10.3.15 IEEE Standard 7-4.3.2, Clause 5.15, Reliability

Requirement: *NOTE—See Annex F for more information about the reliability criterion.*

In addition to the requirements of IEEE Standard 603-1998, when reliability goals are identified, the proof of meeting the goals shall include the software. The method for determining reliability may include combinations of analysis, field experience, or testing. Software error recording and trending may be used in combination with analysis, field experience, or testing.

Per Enclosure B of DI&C-ISG-06 (Reference 15), the reliability analysis is to be supplied with the Phase 2 LAR, and will not be provided herein. The reliability analysis methodology will be consistent with that described in Section 6 of the LTR (Reference 1) as modified by LTR Supplement 1 (Reference 1(c)). The reliability analysis will provide the basis for concluding that Section 5.3.14 of the LTR (Reference 1) remains valid for the CGS PRNM system. [[

]]

10.4 IEEE Standard 7-4.3.2, Clause 6, Sense and Command Features

Requirement: *No requirements beyond IEEE Standard 603-1998 are necessary.*

Per DI&C-ISG-06, Section D.10.4.3 (Reference 15), "There are no criteria beyond those in IEEE Standard 603-1991. Therefore, this clause should be addressed by the review performed under Section D.9.4.3." No further analysis is required in this section.

10.5 IEEE Standard 7-4.3.2, Clause 7, Execute Features

Requirement: *No requirements beyond IEEE Standard 603-1998 are necessary.*

Per DI&C-ISG-06, Section D.10.4.4 (Reference 15), "There are no criteria beyond those in IEEE Standard 603-1991. Therefore, this clause should be addressed by the review performed under Section D.9.4.4." No further analysis is required in this section.

10.6 IEEE Standard 7-4.3.2, Clause 8, Power Source

Requirement: *No requirements beyond IEEE Standard 603-1998 are necessary.*

Per DI&C-ISG-06 (Reference 15), Section D.10.4.5, "There are no criteria beyond those in IEEE Standard 603-1991. Therefore, this clause should be addressed by the review performed under Section D.9.4.5." No further analysis is required in this section.

11. Secure Development and Operational Environment

11.1 Introduction

Information presented in this section is provided to address the requirements of Section D.12.2 of DI&C-ISG-06 (Reference 15) in order for the NRC staff to evaluate the SDOE Controls system integrity.

11.2 Overview

Section 11.4 identifies those concerns that formed the basis for adoption of design features for the CGS PRNM system to protect against undesirable behavior of connected systems and inadvertent access to the system. Section 11.5 addresses the SDOE controls employed for the PRNM system to mitigate the consequences of undesirable behavior of connected systems and inadvertent access to the system.

11.3 Regulatory Evaluation

GDC 21, "Protection system reliability and testability", requires in part that "The protection system shall be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed."

10 CFR 50.55a(h) requires that protection systems for nuclear power plants meet the requirements of IEEE Standard 603-1991, "Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995. With respect to the use of computers in safety systems, IEEE Standard 7-4.3.2-2003 specifies computer-specific requirements to supplement the criteria and requirements of IEEE Standard 603. IEEE Standard 7-4.3.2 reflects advances in digital technology and represents a continued effort by IEEE to support the specification, design, and implementation of computers in safety systems of nuclear power plants. In addition, IEEE Standard 7-4.3.2-2003 specifies computer-specific criteria to supplement the criteria and requirements which are endorsed by RG 1.152.

IEEE Standard 603-1991 Clause 4.8 requires that the design basis shall document as a minimum: "The conditions having the potential for functional degradation of safety system performance and for which provisions shall be incorporated to retain the capability for performing the safety functions (for example, missiles, pipe breaks, fires, loss of ventilation, spurious operation of fire suppression systems, operator error, failure in non-safety-related systems)." Furthermore, IEEE Standard 603-1991 Clause 5.5, "System Integrity," states, "The safety systems shall be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis."

IEEE Standard 603-1991 in Clause 5.6.3.1(2) under Interconnected Equipment states, "No credible failure on the non-safety side of an isolation device shall prevent any portion of a safety system from meeting its minimum performance requirements during and following any DBE requiring that safety function. A failure in an isolation device shall be evaluated in the same manner as a failure of other equipment in a safety system." NRC staff should review the

interconnected systems and equipment to conclude that the safe operation of the system will not be adversely effected due to undesirable behavior of any interconnected systems or equipment.

IEEE Standard 603-1991 in Clause 5.9 under Control of Access states, "The design shall permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof." NRC staff should review the control of access requirements to ensure reliable performance of the safety function.

11.4 Vulnerability Assessment

11.4.1 Connected Systems

The following paragraphs describe the "connected systems" to the PRNM system in order to assess potential vulnerabilities to undesirable behavior of connected systems and inadvertent access to the PRNM system during all phases of the project including both development and operations. These include a discussion of the electrical and data interface methods for all connected systems (Reference 1, Section 5.3.5).

[[

]]

11.4.2 Vulnerability Concern

The potential vulnerabilities during all phases of the project, including both development and operations, can be divided into the following general elements (Reference 1, Section 6.4.3):

[[

]]

11.5 Secure Development and Operational Environment Controls

Per Regulatory Guide 1.152 Revision 3 (Reference 104), the establishment of a SDOE for digital safety systems refers to: (1) measures and controls taken to establish a secure environment for development of the digital safety system against undocumented, unneeded and unwanted modifications and (2) protective actions taken against a predictable set of undesirable acts (e.g., inadvertent operator actions or the undesirable behavior of connected systems) that could challenge the integrity, reliability, or functionality of a digital safety system during operations. These SDOE actions may include adoption of protective design features into the digital safety system design to preclude inadvertent access to the system and/or protection against undesirable behavior from connected systems when operational.

The security, change control and configuration management within the GEH processes ensures that only GEH authorized personnel would have access to the digital safety system under development.

Various protective actions are used to provide controls in assuring SDOE for the CGS PRNM system. Details of the protective actions used in the PRNM system addressing the concerns above are as follows:

11.5.1 Unexpected Response to External "Inputs"

[[

]]

11.5.2 Unexpected Results of Internal Processing

[[

]]

11.5.3 Failure to Execute Correctly the Intended Design

[[

]]

11.5.4 Unauthorized access to the instrument

[[

]]

11.5.5 Address Regulatory Positions 2.1 through 2.5 in Regulatory Guide 1.152 Revision 2

The protective actions and design features described above provide a secure development environment for all phases from design concept through acceptance testing and a secure operation environment so that undocumented code, malicious code, or other unwanted and undocumented features will not inadvertently get incorporated into the system and affect its

safety functions. Table 11-1 addresses SDOE Controls of Regulatory Positions 2.1, Concepts Phase, through 2.5, Test Phase, of Regulatory Guide 1.152, Revision 2 (Reference 46).

11.5.6 Operational Experience

The NUMAC PRNM system as described in NRC approved Reference 1 and various other NUMAC equipment which has the same hardware/software platform and architecture, are operating in numerous BWRs for more than two decades with over 10000 years of operating experience. There are no adverse reports on NUMAC equipment due to undesirable behavior of connected systems, inadvertent access to the system, or network connectivity from any of those plants nor are there any reports of incorporation of undocumented code, malicious code, or other unwanted and undocumented features.

Table 11-1 Correlation of PRNM Design Process to Regulatory Positions 2.1 through 2.5 in Regulatory Guide 1.152 Revision 2

C. Regulatory Position	NUMAC PRNM Design Process
2. Security	[[
2.1 Concepts Phase	
2.2 Requirements Phase 2.2.1 System Features 2.2.2 Development Activities	

2.3 Design Phase 2.3.1 System Features 2.3.2 Development Activities	
2.4 Implementation Phase 2.4.1 System Features 2.4.2 Development Activities	

2.5 Test Phase 2.5.1 System Features 2.5.2 Development Activities	]]

12. References

1. (a) NEDC-32410P-A Volume 1, "Nuclear Measurement Analysis and Control Power Range Neutron Monitor (NUMAC PRNM) Retrofit Plus Option III Stability Trip Function," October 1995.

   (a) NEDC-32410P-A Volume 2 -- Appendices, "Nuclear Measurement Analysis and Control Power Range Neutron Monitor (NUMAC PRNM) Retrofit Plus Option III Stability Trip Function," October 1995.

   (b) NEDC-32410P-A, Supplement 1, "Nuclear Measurement Analysis and Control Power Range Neutron Monitor (NUMAC PRNM) Retrofit Plus Option III Stability Trip Function," November 1997.

2. (a) NRC letter to Mr. David W. Reigel, NUMAC Project Manager, "Acceptance of Licensing Topical Report NEDC- 32410-P, Nuclear Measurement Analysis and Control Power Range Neutron Monitor (NUMAC-PRNM) Retrofit Plus Option III Stability Trip Function (TAC No. M90616)," September 5, 1995.

   (a) NRC letter to Mr. David W. Reigel, NUMAC Project Manager, *Licensing Topical Report NEDC- 32410-P, Supplement 1, Nuclear Measurement Analysis and Control Power Range Neutron Monitor (NUMAC-PRNM) Retrofit Plus Option III Stability Trip Function (TAC No. M95746)*, August 15, 1997.

3. NUREG-1433, "Standard Technical Specifications General Electric Plants, BWR/4 Specifications," Revision 3, dated June 2004. (ML041910211).

4. GE Hitachi Nuclear Energy, " Columbia Generating Station Power Range Neutron Monitoring System Architecture & Theory of Operations Report," NEDC-33696P, Revision 0, November 2011.

5. GE Hitachi Nuclear Energy, "PRNM Requirements Specification," 24A5221TC, Revision 6, dated March 18, 2010.*

6. GE Nuclear Energy, "Nuclear Energy Business Group Boiling Water Reactor Quality Assurance Program Description (Revision 4)," NEDO-11209-04A, December 31, 1982.

7. GE Nuclear Energy, "GE Nuclear Energy Quality Assurance Program Description," NEDO-11209-04A (Revision 8), dated March 31, 1989.

8. GE Nuclear Energy, "ISO-9001 Quality Management System Description," NEDO-33280, Revision 9.

9. GE Hitachi Nuclear Energy, "GE Hitachi Nuclear Energy Quality Assurance Program Description," NEDO-11209, Revision 9, dated December 9, 2010.

10. Final Safety Evaluation for GEH Topical Report NEDO-11209, Revision 9, "GE Hitachi Nuclear Energy Quality Assurance Program Description," dated August 8, 2011. (ML112140604).

11. GE Hitachi Nuclear Energy, "Columbia Generating Station Power Range Neutron Monitoring System Response Time Analysis Report," NEDC-33690P, Revision 0, dated November 2011.

12. NRC BTP 7-21, "Guidance on Digital Computer Real-time Performance," (ADAMS Accession No. ML070550070).

13. Digital I&C-ISG-04, "Task Working Group #4: Highly Integrated Control Rooms-Communications Issues," Revision 1, dated March 6, 2009.

14. GE Hitachi Nuclear Energy, "Columbia Generating Station Plant-Specific Responses Required by NUMAC PRNM Retrofit Plus Option III Stability Trip Function Topical Report (NEDC-32410P-A)," 0000-0101-7647-R3, dated November 2011.

15. Digital I&C-ISG-06, "Task Working Group #6: Licensing Process," Revision 1, dated January 19, 2011 (ADAMS Accession No, ML110140103).

16. EOP 25-5.00, Work Planning and Scheduling.

17. P&P 10-29, Project Risk Management Procedure.

18. P&P 70-11, Quality System Requirements.

19. P&P 70-14, Quality Assurance Audit Requirements.

20. EOP 75-5.00, Quality and Technical Training.

21. EOP 75-6.00, Quality Assurance Records.

22. CP-16-01, Corrective Action Process.

23. CP-18-101, Self-Assessment Program.

24. EOP 75-4.00, Material Inspection and Release.

25. EOP 30-3.40, Product Data Management System.

26. EOP 42-8.00, Document Initiation or Change by ERM/ECN.

27. EOP 42-10.00, Design Record File.

28. EOP 55-2.00, Engineering Change Control.

29. CP-03-09, Independent Design Verification.

30. EOP 65-2.20, Customer Purchase Order Technical Evaluations and Dedication of Commercial Grade Items.

31. EOP 75-4.30, Customer Supplied Material.

32. CP-04-107, Order Placement.

33. CP-03-04, Technical Reviews

34. NUMAC Software Verification and Validation Plan, 23A5163, Revision 3.*

35. IEEE Standard 1012, "IEEE Standard for Software Verification and Validation," 1998.

36. NRC BTP 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems."

37. Entergy Letter, "Responses to NRC Requests for Additional Information Pertaining to License Amendment Request for Power Range Neutron Monitoring System (TAC No. ME2531)," GNRO-2011/00039, dated May 26, 2011 (ML111460590).

38. Entergy Letter, "Responses to NRC Requests for Additional Information Pertaining to License Amendment Request for Power Range Neutron Monitoring System (TAC No. ME2531)," GNRO-2011/00038, dated May 16, 2011 (ML111370259).

39. Entergy Letter, "Responses to NRC Requests for Additional Information Pertaining to License Amendment Request for Power Range Neutron Monitoring System (TAC No. ME2531)," GNRO-2011/00032, dated May 3, 2011 (ML111230756).

40. Entergy Letter, "Response to NRC Requests for Additional Information Pertaining to License Amendment Request for Power Range Neutron Monitoring System (TAC No. ME2531)," GNRO-2011/00057, dated July 22, 2011 (ML112061524).

41. GEH Nuclear Energy, "NUMAC Software Configuration Management Plan," 23A5161, Revision 4.*

42. NUMAC Software Management Plan, 23A5162, Revision 3.*

43. IEEE Standard 1074, "IEEE Guide for Developing Software Life Cycle Processes," 1995.

44. NRC RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 0, 1997.

45. IEEE Standard 7-4.3.2, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," 2003.

46. NRC RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Revision 2, 2006.

47. NUMAC Requirements Specification, 23A5082, Revision 1.*

48. NUMAC Power Range Neutron Monitoring System Requirements Specification, 24A5221, Revision 17.*

49. Software Conventions and Guidelines, 26A5410, Revision 0.

50. NUREG/CR-6463, "Review Guidelines on Software Languages for Use in nuclear Power Plant Safety Systems."

51. NRC RG 1.28, "Quality Assurance Program Criteria (Design and Construction)," Revision 3.

52. IEEE Standard 730, "IEEE Standard for Software Quality Assurance Plans," 1998.

53. NUREG/CR-6101, "Software Reliability and Safety in Nuclear Reactor Protection Systems."

54. EOP 75-7.00, Statistical Techniques.

55. GE Nuclear Energy, "Technical Specification Improvement Analysis for BWR Reactor Protection System," NEDC-30851P-A, March 1988.

56. EPRI NP-2230.

57. NRC RG 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 1, 2004.

58. IEEE Standard 828, "IEEE Standard for Software Configuration Management Plans," 1990.

59. NRC RG 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," 1997.

60. IEEE Standard 829, "IEEE Standard for Software Test Documentation," 1983.

61. NRC RG 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," 1997.

62. IEEE Standard 1008, "IEEE Standard for Software Unit Testing," 1987.

63. NRC RG 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," 1997.

64. APRM Performance Specification, 25A5916, Revision 5.*

65. APRM Performance Specification Data Sheet, 25A5916TC, Revision 4.*

66. IEEE Standard 830, "IEEE Recommended Practice for Software Requirements Specifications," 1993.

67. NRC RG 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," 1997.

68. APRM Functional Software Design Specification, 26A6774, Revision 1.*

69. APRM Functional Software Design Specification Data Sheet, 26A6774TC, Revision 1.*

70. NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition."

71. IEEE Standard 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," 1991.

72. GEH Nuclear Energy, "NUMAC PRNM Components 268X1331TCG001, 268X1332TCG001, G002 268X1333TCG001 Qualification Summary for Energy Northwest, CGS," Revision 1, November 8, 2010.

73. GE Hitachi Nuclear Energy, "Energy Northwest Columbia Generating Station, Seismic Qualification of NUMAC Power Range Neutron Monitoring (PRNM) System Equipment Control Panel", 0000-0106-7539, Revision 1, September 2010.

74. IEEE Standard 323, "IEEE Standard for Qualifying Class IE Equipment for Nuclear Power Generating Stations," 1974.

75. IEEE Standard 344, "IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations," 1975.

76. NRC RG 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," Revision 1, 2003.

77. EPRI-TR-102323, "Guidelines for Electromagnetic Interference Testing in Power Plants," Revision 2, 2000.

78. MIL-STD-461E, "Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment."

79. EPRI-TR-102323, "Guidelines for Electromagnetic Interference Testing in Power Plants," Revision 0, 1994.

80. EPRI-TR-102348, "Guideline on Licensing Digital Upgrade," Revision 1.

81. EPRI TR-102323, "Guidelines for Electromagnetic Interference Testing of Power Plant Equipment," Revision 3, 2004.

82. GEH Nuclear Energy, "Columbia Generating Station Power Range Neutron Monitor System Diversity and Defense-in-Depth (D3) Analysis," NEDC-33694P, Revision 1, January 2012.

83. NRC BTP 7-19, "Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems," (ADAMS Accession No. ML093490771).

84. GE Hitachi Nuclear Energy, "Columbia Generating Station Power Range Neutron Monitoring Design Analysis Report, NEDC-33697P, Revision 1, January 2012.

85. GE Hitachi Nuclear Energy, "Energy Northwest Columbia Generating Station APRM/RBM/Technical Specifications/Maximum Extended Load Line Limit Analysis (ARTS/MELLLA)," NEDC-33507P, Revision 0, April 2010.

86. IEEE Standard 279, "Criteria for Protection Systems for Nuclear Power Generating Stations," 1971.

87. IEEE Standard 323, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," 1983.

88. GE Hitachi Nuclear Energy, "Columbia Generating Station Power Range Neutron Monitoring System Design Report on Computer Integrity, Test and Calibration, and Fault Detection," NEDC-33698, Revision 2, dated December 2012.

89. GE Hitachi Nuclear Energy, "NUMAC Power Range Neutron Monitor (PRNM) Panel and System Separation Analysis Columbia Generating Station (CGS)", Revision 1 (DRF Section 0000-0106-7482).

90. NRC RG 1.75, "Physical Independence of Electric Systems," Revision 2, 1978.

91. IEEE Standard 384, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits," 1974.

92. IEEE Standard 384, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits," 1981.

93. IEEE Standard 384, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits," 1992.

94. APRM User Manual, 26A7865, Revision 4, September 4, 2010.

95. APRM ODA User's Manual, 26A7868, Revision 1, dated February 20, 2010.

96. NUREG-0700, "Human-System Interface Design Review Guidelines."

97. GE Nuclear Energy, "General Electric Instrument Setpoint Methodology," NEDC-31336P-A, September 1996 (NRC Accession Number ML072950103).

98. NRC RG 1.105, "Setpoints for Safety-Related Instrumentation," Revision 2, 1986.

99. NRC RG 1.105, "Setpoints for Safety-Related Instrumentation," Revision 3, 1999.

100. GE Hitachi Nuclear Energy Report, "Instruments Limits Calculation, ENERGY NORTHWEST Columbia Generating Station, Average Power Range Monitor, Power Range Neutron Monitoring System (NUMAC-ARTS/MELLLA)," 0000-0112-7649-R1, Revision 1, March 2010.

101. NEDO-32465-A, "Licensing Topical Report, Reactor Stability Detect and Suppress Solutions Licensing Basis Methodology for Reload Applications, Licensing Topical Report," Class I, August 1996.

102. TVA to NRC, "Browns Ferry Nuclear Plant (BFN) - Unit 1, Technical Specifications (TS) Change TS-3 - Request for Additional Information (RAI) Regarding Oscillation Power Range Monitor (OPRM) - (TAC No. MC9565)," NA-BFN-TS-443, October 2, 2006.

103. MNGP to NRC, "Response to Requests for Additional Information for License Amendment Request for Power Range Neutron Monitoring System Upgrade (TAC No. MD8064), September 16, 2008.

104. NRC RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Revision 3, 20011.

* References 5, 34, 41, 42, 47, 48, 64, 65, 68, and 69 have been included in Appendix A.