LICENSE AMENDMENT REQUEST TO CHANGE TECHNICAL SPECIFICATIONS IN SUPPORT OF PRNM AND ARTS / MELLLA IMPLEMENTATION
Enclosure 2 – Attachment 12

NEDO-33697, Revision 1

Columbia Generating Station Power Range Neutron Monitoring System Design Analysis Report

January 2012

(non-proprietary version)

HITACHI

GE Hitachi Nuclear Energy

NEDO-33697
Revision 1
DRF Section 0000-0139-4778 R2
January 2012

Non-Proprietary Information-Class I (Public)

Columbia Generating Station
Power Range Neutron Monitoring System
Design Analysis Report

Information Notice

This is a non-proprietary version of the document NEDC-33697P, Revision 1, 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 THE 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 of NEDC-33685P and NEDC-33694P (Enclosure 1).

Table of Contents

ACRONYMS AND ABBREVIATIONS

Term	Definition
ABA	Amplitude Based Algorithm
A/D	Analog/Digital
AGAF	APRM Gain Adjustment Factor
APRM	Average Power Range Monitor
AR	As Required
ARTS	Average Power Range Monitor, Rod Block Monitor Technical Specification Improvement Program
ASP	Automatic Signal Processor
ATWS	Anticipated Transient Without Scram
BTP	Branch Technical Position
CAL	Calibrate
CCF	Common-Cause Failure
CGS	Columbia Generating Station
CMOS	Complementary Metal-Oxide Semiconductor
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CTP	Core Thermal Power
D/A	Digital/Analog
DI&C-ISG	Digital I&C Interim Staff Guidance
DMA	Direct Memory Access
DRF	Design Record File
DSS-CD	Detect and Suppress Solution-Confirmation Density
EEPROM	Electrically Erasable Programmable Read-Only Memory
EMC	Electromagnetic Compatibility
ENW	Energy Northwest
EPRI	Electric Power Research Institute
EPROM	Electronic-Programmable Read-Only Memory
FAT	Factory Acceptance Testing
FDI	Field Disposition Instruction
FDDI	Fiber Direct Data Interface
FMEA	Failure Modes and Effects Analysis

Term	Definition
FO	Fiber Optic
FRD	Firmware Release Description
GAF	Gain Adjustment Factor
GEDAC	General Electric Data Acquisition & Communication
GEH	GE-Hitachi Nuclear Energy Americas LLC
GEIO	General Electric Input Output
GGNS	Grand Gulf Nuclear Station
GRBA	Growth Rate Based Algorithm
HDL	High Density Logic
HICR	Highly-Integrated Control Room
HVPS	High Voltage Power Supply
IEEE	Institute of Electrical and Electronics Engineers
I&C	Instrumentation & Controls
IC	Integrated Circuit
INOP	Inoperable
I/O	Input/Output
IO	Input Output
ISG	Interim Staff Guidance
I/V	Current-Voltage
LAR	License Amendment Request
LPRM	Local Power Range Monitor
LTR	Licensing Topical Report
MCR	Main Control Room
MELLLA	Maximum Extended Load Line Limit Analysis
NIC	NUMAC Interface Computer
NRC	Nuclear Regulatory Commission
NUMAC	Nuclear Measurement Analysis and Control
NUREG	Nuclear Regulatory Commission Regulation
NVRAM	Non-Volatile Random Access Memory
ODA	Operator Display Assembly
ODIO	Open Drain Input/Output

Term	Definition
OP AMP	Operational Amplifier
OPER	Operate
OPRM	Oscillation Power Range Monitor
OS	Operating System
PCI	Power Range Communication Interface
PDMS	Product Data Management System
PL	Programmable Logic
PLD	Programmable Logic Device
PPC	Primary Plant Computer
PRNM	Power Range Neutron Monitor
PRNMS	Power Range Neutron Monitoring System
PVCS	Polytron Version Control System
PWB	Printed Wire Board
RAI	Request for Additional Information
RAM	Random Access Memory
RBM	Rod Block Monitor
RCCE	Responsible Configuration Control Engineer
RE	Responsible Engineer
RG	Regulatory Guide
RM	Responsible Manager
RMCS	Reactor Manual Control System
RPS	Reactor Protection System
RRCS	Redundant Reactivity Control System
SCMP	Software Configuration Management Plan
SER	Safety Evaluation Report
SLC	Standby Liquid Control
SLO	Single Loop Operation
SMP	Software Management Plan
SOE	Sequence of Event
SRAM	Static Random Access Memory
SRI	Select Rod Insert

Term	Definition
ST	Standard Style
STP	Simulated Thermal Power
SVVP	Software Verification and Validation Plan
TOPPS	Thermal Over Power Protection System
TR	Topical Report
TRA	Transient Recording Analysis
US	United States
V&V	Verification and Validation

1. Introduction

This Design Analysis Report has been generated as a Digital Instrumentation & Control-Interim Staff Guidance (DI&C-ISG)-06 Phase 1 deliverable to support the license amendment request (LAR) submittal for the Columbia Generating Station (CGS) Power Range Neutron Monitoring System (PRNMS).

1.1. Scope

The scope of this Design Analysis Report is based upon, and addresses, the following sections of DI&C-ISG-06 Revision 1:

- D.7 Communications (D.7.2)
- D.8 System, Hardware, Software, and Methodology Modifications (D.8.2)
- D.9.4.2.6 Institute of Electrical and Electronics Engineers (IEEE) Standard 603, Clause 5.6, Independence
- D.10.4.2.6 IEEE Standard 7-4.3.2, Clause 5.6, Independence

The information requested within each of these DI&C-ISG-06 sections is addressed within the content of this report.

1.2. Report Structure

This report has been structured to ensure that reviewers can quickly and effectively identify and understand the information provided for each specific DI&C-ISG-06 section within the scope of this report.

This report is divided into the following sections:

- Section 2, Communications
- Section 3, System, Hardware, Software, and Methodology Modifications
- Section 4, IEEE Standard 603 Clause 5.6, Independence
- Section 5, IEEE Standard 7-4.3.2 Clause 5.6, Independence

To ensure the clarity of the information provided to reviewers within the body of this report, specific detailed information is provided in the following enclosures – which are referenced within the applicable sections of this report:

- Enclosure 1, DI&C-ISG-04 Compliance
- Enclosure 2, CGS PRNMS Hardware, Software, and Software Development Changes

2. Communications

DI&C-ISG-06, Section D.7.2 states the following:

> The licensee's submittal should provide sufficient documentation to support and justify the ability of the digital I&C system to limit the effect of a failed channel from adversely affecting separate channels or divisions. The documentation should provide sufficient justification to allow the conclusion that the plan meets the standards of IEEE Std 603-1991 Clause 5.6, IEEE Std 7-4.3.2 Clause 5.6, and BTP 7-11. Typically, this involves a detailed discussion of where communications are possible, the nature of those communications, and the features of the system that provide the ability to preclude or account for errors.
>
> The information to confirm adequate data isolation should be contained in the system, hardware and software specifications, architecture, and descriptions. Depending on the complexity of the proposed communications, the NRC staff also may have to examine the actual circuitry as described in the circuit schematics and in the software code listings, and in detailed system and hardware drawings. The licensee should provide documentation on how each clause in DI&C-ISG-04 has been met, or what alternative and proposed alternatives when an individual clause is not met.

The following provides a summary description of how the CGS PRNM addresses the above, and identifies the individual documents/sections which provide detailed descriptions and detailed information.

[[

]]

[[

]]

Figure 6 (from NEDC-33696P). PRNM System-Level Architecture

NEDC-33696P (Reference 2) also provides detailed descriptions of each of these pathways which address potential concerns related to:

- [[

]]

IEEE Standard 603-1991 Clause 5.6 is addressed below in Section 4, IEEE Standard 603 Clause 5.6, Independence.

IEEE Standard 7-4.3.2, Clause 5.6 is addressed below in Section 5, IEEE Standard 7-4.3.2 Clause 5.6, Independence

The DI&C-ISG-04 clauses are addressed in Enclosure 1, DI&C-ISG-04 Compliance.

3. System, Hardware, Software, and Methodology Modifications

The information identified in D.8.2 of DI&C-ISG-06 is addressed in two parts as noted below.

3.1. Deviations & Changes from Previously Approved Licensing Topical Report

The first part of DI&C-ISG-06 D.8.2 states:

> The information provided should identify all deviations to the system, hardware, software, or design lifecycle methodology from a previous NRC approval of a digital I&C system or approved topical report. The intent is to eliminate NRC staff reviews of items that have been reviewed and approved, and also to allow the NRC staff to conclude that any changes do not invalidate conclusions reached by a previous review. Completion of this review should result in an update of the previous digital I&C system; however, for topical reports (TRs), it is strongly encouraged that the updated TRs be submitted for approval before a LAR is submitted referencing the TR.

The CGS PRNM system has been designed in accordance with the previously approved Licensing Topical Report (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 3. Changes made to the original design (Hatch in 1997) that appear in the CGS platform are provided in Enclosure 2, CGS PRNMS Hardware, Software, & Software Development Changes, of this report. Note that the changes provided in Enclosure 2 do not deviate from the PRNM requirements approved in the LTR.

3.2. Review of Enclosure B Documents

The second part of DI&C-ISG-06, Section D.8.2 states:

> Where appropriate, the licensee and vendor should discuss each of the documents listed in Enclosure B of this ISG. For each document, the licensee and vendor should state whether this document has changed since the last review. If the document has not changed, the licensee and vendor should show the date when the document was previously submitted, and the ADAMS accession number where the document can currently be found. For documents, including system, hardware and software descriptions that have changed, the licensee should submit, on the docket, the new version of that document. In cases where the changes are minor, the licensee can choose to submit a description of the change. The information provided should provide adequate justification to allow the NRC staff to evaluate the acceptability of the change. Additionally, the licensee should justify how the pertinent features of the subject plant conform to those of the existing approval. The amount of information should be proportional to the significance of the change.

As noted in Section 3.1, deviations from the LTR are listed in Enclosure 1 of Reference 3. Enclosure 2, CGS PRNMS Hardware, Software, & Software Development Changes, includes changes from the first PRNM system installed in the United States (Hatch, 1997), which is identical to the platform described in Reference 1.

The documents generated to address the Phase 1 submittals listed in Enclosure B have not been previously submitted as distinct documents. Therefore, this part of D.8.2 is not applicable to the CGS PRNM project.

4. IEEE Standard 603 Clause 5.6, Independence

The Physical and Electrical Independence, and Communication Independence aspects of Clause 5.6 of IEEE Standard 603 are addressed separately in the following two sub-sections.

4.1. Physical and Electrical Independence

The first part of DI&C-ISG-06, Section D.9.4.2.6 states:

> Clause 5.6 requires independence between (1) redundant portions of a safety system, (2) safety systems and the effects of design bases events, and (3) safety systems and other systems[5]. [*Text of footnote 5 below*]
>
> [5] An independence design analysis report provides sufficient detail to support and justify independence: (1) between redundant portions of a safety systems, (2) from the effects of design basis events, and (3) from other systems. Some of the supporting analysis is sometimes documented in a Failure Modes and Effects Analysis (FMEA) report; see Section D.9.4.2.1.1.]
>
> Guidance for evaluation of physical and electrical independence is provided in RG 1.75, Revision 3, "Criteria for independence of Electrical Safety Systems," which endorses IEEE Standard 384-1992, "IEEE Standard Criteria for independence of Class 1E Equipment and Circuits." The safety system design should not have components that are common to redundant portions of the safety system, such as common switches for actuation, reset, mode, or test; common sensing lines; or any other features that could compromise the independence of redundant portions of the safety system. Physical independence is attained by physical separation and physical barriers. Electrical independence is attained by physical separation and physical barriers. Electrical independence should include the utilization of separate power sources. Transmission of signals between independent channels should be through isolation devices.

The requirements of IEEE Standard 603 Clause 5.6 and its sub-clauses are addressed by the responses provided in NEDC-33685P (Reference 4), Section 9.2.6.

As documented in NEDC-33685P (Reference 4), the requirements for physical and electrical independence defined in IEEE Standard 603 Clause 5.6.1 are addressed by the physical and electrical separation described and supplemented in the LTR (Reference 1), based on IEEE Standard 279-1971.

In addition, as also noted in Reference 4, an independent NUMAC PRNM panel and system separation analysis was conducted for CGS. Based upon the results of that analysis, GEH concluded that: "*the design of the PRNM panel assures that no credible single failure, internal or external to the PRNM panel, will result in loss of the APRM or OPRM trip functions, and that the effects of single failures in the PRNM panel will be equal to or less severe on external circuits compared to the original PRNM design.*"

4.2. Communications Independence

The second part of DI&C-ISG-06, Section D.9.4.2.6 states:

> SRP Chapter 7, Appendix 7.1-C, Section 5.6, "Independence," 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 function of the redundant portions. Further, 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 must not be able to affect the functions of the safety system. Section D.7 and DI&C-ISG-04 provide additional information on this topic.

Communication independence as related to the requirements of IEEE Standard 603 Clause 5.6 is addressed within Reference 4, as noted above.

Section 2, Communications, above provides a summary description and overview of the PRNM data communication links and pathways. As noted within that overview, detailed descriptions of each of these pathways are provided in NEDC-33696P (Reference 2).

As also noted in Section 2, DI&C-ISG-04 is addressed in Enclosure 1 of this report.

5. IEEE Standard 7-4.3.2 Clause 5.6, Independence

DI&C-ISG-06, Section D.10.4.2.6 states the following:

> Clause 5.6 specifies that in addition to the requirements of IEEE Std 603-1991, 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.

As noted above in Section 4, IEEE Standard 603 Clause 5.6, Independence, the independence of data communication has been included within the discussion found in NEDC-33685P, Reference 4.

The data communication between safety channels and between safety and non-safety systems summarized above in Section 2, Communications, and described in detail in the NEDC-33696P (Reference 2) demonstrate that the requirements of IEEE Standard 7-4.3.2 Clause 5.6 have been satisfied.

DI&C-ISG-04 is addressed within Enclosure 1 of this report.

6. References

1. (a) GE Nuclear Energy, "Nuclear Measurement Analysis and Control Power Range Neutron Monitor (NUMAC PRNM) Retrofit Plus Option III Stability Trip Function," NEDC-32410P-A, Volume 1 & 2, October 1995 (ADAMS Accession No. ML9605290009); and

   (b) GE Nuclear Energy, "Nuclear Measurement Analysis and Control Power Range Neutron Monitor (NUMAC PRNM) Retrofit Plus Option III Stability Trip Function," NEDC-32410P-A, Supplement 1, November 1997 (ADAMS Accession No. ML9806120242).

2. GE Hitachi Nuclear Energy, "Columbia Generating Station Power Range Neutron Monitoring System Architecture & Theory of Operations Report," NEDC-33696P, Revision 0, November 2011.

3. 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.

4. GE Hitachi Nuclear Energy, "Digital I&C-ISG-06 Compliance for Columbia Generating Station NUMAC Power Range Neutron Monitoring Retrofit Plus Option III Stability Trip Function," NEDC-33685P, Revision 1, January 2012.

Enclosure 1

DI&C-ISG-04 Compliance

Table of Contents

1. Introduction & Background

The purpose and intent of this attachment is to ensure that Nuclear Regulatory Commission (NRC) staff reviewers:

a) are provided sufficient information to demonstrate that the CGS PRNM system satisfies the criteria of the staff positions defined within DI&C ISG-04; and

b) that the information is presented in a manner which facilitates their review.

As discussed below under the Background subsection, DI&C-ISG-04 Compliance Matrices for both the CGS and Grand Gulf Nuclear Station (GGNS) PRNM systems have previously been submitted to the NRC in response to the NRC requests for supplemental and additional information respectively.

The CGS and GGNS matrices, with some minor exceptions, addressed the DI&C-ISG-04 staff positions using the same information. This information, as noted in GGNS request for additional information (RAI) 12 through 19, was not sufficient to demonstrate staff positions had been satisfied.

Given the commonalities between the GGNS and CGS PRNM systems, the DI&C-ISG-04 compliance matrix issues which had to be addressed for the GGNS PRNM system, must also be addressed for the CGS PRNM system. However, incorporating the information to address those issues into a new and expanded CGS matrix would necessitate a complete re-review and evaluation of the entire matrix.

To facilitate the review, the issues raised within each of the GGNS RAIs – as they apply to equipment and architecture of the CGS PRNM system have been addressed independently in Section 3, Supplemental Information.

Section 2, CGS DI&C-ISG-04 Compliance Matrix, contains the CGS DI&C-ISG-04 compliance matrix previously submitted in Reference 1.

While the original information has not been revised, the staff positions for which the GGNS RAIs identified the information as being insufficient have been shaded in yellow and annotated to identify the specific sections providing supplemental information.

Background

In response to an NRC request for supplement information to demonstrate the CGS PRNM upgrade's compliance to DI&C-ISG-04, a CGS DI&C-ISG-04 Compliance Matrix was developed and submitted in Reference 1.

As the NRC's review of the CGS PRNM LAR application "concluded that it did not provide technical information in sufficient detail to enable the NRC staff to complete its detailed review," the adequacy of the responses provided in the submitted CGS DI&C-ISG-04 Compliance Matrix was not established at that time.

A similar request was transmitted in RAI 4 (Reference 2). The information which had been developed for the CGS PRNM was incorporated into a GGNS PRNM DI&C-ISG-04 compliance matrix and submitted in Attachment 3 to Reference 3.

References:

1. Energy Northwest, "Columbia Generating Station, Docket No. 50-397 Response to Request for Supplemental Information for Completion of Acceptance Review for PRNM/ARTS/MELLLA System Upgrade," G02-10-099, dated July 30, 2010 (ADAMS Accession No. ML102360357).
2. NRC Letter, "Grand Gulf Nuclear Station, Unit 1 - Request for Additional Information Re: Power Range Neutron Monitoring System (TAC No. ME2531)," GNRI-2010/00067, dated May 4, 2010 (ADAMS Accession No. ML101190125).
3. Entergy Letter, "Responses to NRC Requests for Additional Information Pertaining to License Amendment Request for Power Range Neutron Monitoring System (TAC No. ME2531)," GNRO-2010/00040, dated June 3, 2010 (ADAMS Accession No. ML101790436).

2. CGS DI&C-ISG-04 Compliance Matrix

CGS DI&C-ISG-04 Compliance Matrix

	DI&C-ISG-04 Text/Guidance	CGS PRNM Conformance to DI&C-ISG-04
1.	**Scope:**	
2.	Design and review of digital systems proposed for safety related service in nuclear power plants	This statement is not a requirement.
3.	Does not apply to interactions within the same division of safety related systems	This statement defines the scope but is not a requirement.
4.	Does not apply to non-safety related systems	This statement defines the scope but is not a requirement.
5.	Applies to non-safety related systems that may affect plant conformance to safety analysis (accident analysis, transient analysis)	This statement defines the scope but is not a requirement.
6.	**Definitions:**	
7.	The term "Highly-Integrated Control Room" (HICR) refers to a control room in which the traditional control panels, with their assorted gauges, indicating lights, control switches, annunciators, etc., are replaced by computer-driven consolidated operator interfaces. In an HICR:	The statement is not a requirement but a definition. The following is provided for clarification only. Operator Display Assemblies (ODAs) are provided as part of the PRNM upgrade for displaying PRNM variables and status. The ODAs are not used to control safety functions.
8.	The primary means for providing information to the plant operator is by way of computer driven display screens mounted on consoles or on the control room walls.	The ODAs are generally used as the primary display for some functions; however, most other parameters remain on the main bench board.
9.	The primary means for the operator to command the plant is by way of touch screens, keyboards, pointing devices or other computer-based provisions.	PRNM does not provide capability to operate any plant equipment from the ODA, touch screens, keyboards, pointing devices, or any other computer-based provision.

	DI&C-ISG-04 Text/Guidance	CGS PRNM Conformance to DI&C-ISG-04
10	A digital workstation is in essence just one device. Unlike a conventional control panel, there is no way for its many functions to be independent of or separated from one another, because they all use the same display screen, processing equipment, operator interface devices, etc. Functions that must be independent must be implemented in independent workstations.	Divisional separation is maintained in the PRNM. Displays, whether in the control room (ODA), or on the face of an instrument, are divisional.
11	This ISG describes how controls and indications from all safety divisions can be combined into a single integrated workstation while maintaining separation, isolation, and independence among redundant channels. This ISG does not alter existing requirements for safety-related controls and displays to support manual execution of safety functions.	No comment. Not a requirement.
12	**2.1. Interdivisional Communications**	Not a requirement.
13	**Scope:**	
14	As used in this document, interdivisional communications includes transmission of data and information among components in different electrical safety divisions and communications between a safety division and equipment that is not safety-related. It does not include communications within a single division. Interdivisional communications may be bidirectional or unidirectional.	[[ ]]
15	**STAFF POSITION**	

	DI&C-ISG-04 Text/Guidance	CGS PRNM Conformance to DI&C-ISG-04
16	Bidirectional communications among safety divisions and between safety and nonsafety equipment is acceptable provided certain restrictions are enforced to ensure that there will be no adverse impact on safety systems.	This is a high level guide and compliance is demonstrated by addressing the specific NRC guidance in the following sections.
17	Systems which include communications among safety divisions and/or bidirectional communications between safety division and non-safety equipment should adhere to the guidance described in the remainder of this section. Adherence to each point should be demonstrated by the applicant and verified by the reviewer. This verification should include detailed review of the system configuration and software specifications, and may also involve a review of selected software code.	This is a high level guide and compliance is demonstrated by addressing the specific NRC guidance in the following sections. The reviewer in this document is assumed to be the NRC reviewer.
18	Staff Position 1.1. A safety channel should not be dependent upon any information or resource originating or residing outside its own safety division to accomplish its safety function. This is a fundamental consequence of the independence requirements of IEEE603. It is recognized that division-voting logic must receive inputs from multiple safety divisions.	[[ ]]
19	Staff Position 1.2. The safety function of each safety channel should be protected from adverse influence from outside the division of which that channel is a member.	[[ ]]

	DI&C-ISG-04 Text/Guidance	CGS PRNM Conformance to DI&C-ISG-04
20	Staff Position 1.2 (implementation details). Information and signals originating outside the division must not be able to inhibit or delay the safety function. This protection must be implemented within the affected division (rather than in the sources outside the division), and must not itself be affected by any condition or information from outside the affected division. This protection must be sustained despite any operation, malfunction, design error, communication error, or software error or corruption existing or originating outside the division.	[[ ]]
21	Continuation of response from above.	[[ ]]

	DI&C-ISG-04 Text/Guidance	CGS PRNM Conformance to DI&C-ISG-04
22	Staff Position 1.3. A safety channel should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function. Receipt of information that does not support or enhance the safety function would involve the performance of functions that are not directly related to the safety function. Safety systems should be as simple as possible. Functions that are not necessary for safety, even if they enhance reliability, should be executed outside the safety system. A safety system designed to perform functions not directly related to the safety function would be more complex than a system that performs the same safety function, but is not designed to perform other functions. The more complex system would increase the likelihood of failures and software errors.	[[ ]]
23	Continuation of Staff Position 1.3 from above. Such a complex design, therefore, should be avoided within the safety system. For example, comparison of readings from sensors in different divisions may provide useful information concerning the behavior of the sensors (for example, On-Line Monitoring). Such a function executed within a safety system, however, could also result in unacceptable influence of one division over another, or could involve functions not directly related to the safety functions, and should not be executed within the safety system.	[[ ]]
24	Continuation of response to Staff Position 1.3.	[[ ]]

	DI&C-ISG-04 Text/Guidance	CGS PRNM Conformance to DI&C-ISG-04
25	Continuation of response to Staff Position 1.3.	[[ ]]
26	Staff Position 1.3 (implementation details). Receipt of information from outside the division, and the performance of functions not directly related to the safety function, if used, should be justified. It should be demonstrated that the added system/software complexity associated with the performance of functions not directly related to the safety function and with the receipt of information in support of those functions does not significantly increase the likelihood of software specification or coding errors, including errors that would affect more than one division. The applicant should justify the definition of "significantly" used in the demonstration.	See the above justification. All of the data received by the safety system that does not support a safety function are simple operations and are executed on a lower priority basis than the safety function. This requirement is met.

	DI&C-ISG-04 Text/Guidance	CGS PRNM Conformance to DI&C-ISG-04
27	Staff Position 1.4. The communication process itself should be carried out by a communications processor separate from the processor that executes the safety function, so that communications errors and malfunctions will not interfere with the execution of the safety function. The communication and function processors should operate asynchronously, sharing information only by means of dual-ported memory or some other shared memory resource that is dedicated exclusively to this exchange of information. The function processor, the communications processor, and the shared memory, along with all supporting circuits and software, are all considered to be safety-related, and must be designed, qualified, fabricated, etc., in accordance with 10 CFR Part 50, Appendix A and B. Access to the shared memory should be controlled in such a manner that the function processor has priority access to the shared memory to complete the safety function in a deterministic manner.	[[ ]]

	DI&C-ISG-04 Text/Guidance	CGS PRNM Conformance to DI&C-ISG-04
28	Continuation of Staff position 1.4. For example, if the communication processor is accessing the shared memory at a time when the function processor needs to access it, the function processor should gain access within a timeframe that does not impact the loop cycle time assumed in the plant safety analyses. If the shared memory cannot support unrestricted simultaneous access by both processors, then the access controls should be configured such that the function processor always has precedence. The safety function circuits and program logic should ensure that the safety function will be performed within the timeframe established in the safety analysis, and will be completed successfully without data from the shared memory in the event that the function processor is unable to gain access to the shared memory.	[[ ]]
29	Staff Position 1.5. The cycle time for the safety function processor should be determined in consideration of the longest possible completion time for each access to the shared memory. This longest-possible completion time should include the response time of the memory itself and of the circuits associated with it, and should also include the longest possible delay in access to the memory by the function processor assuming worst-case conditions for the transfer of access from the communications processor to the function processor. Failure of the system to meet the limiting cycle time should be detected and alarmed.	[[ ]]

	DI&C-ISG-04 Text/Guidance	CGS PRNM Conformance to DI&C-ISG-04
30	Staff Position 1.6. The safety function processor should perform no communication handshaking and should not accept interrupts from outside its own safety division.	[[ ]]
31	Staff Position 1.7. Only predefined data sets should be used by the receiving system. Data from unrecognized messages must not be used within the safety logic executed by the safety function processor.	[[ ]]
32	Staff Position 1.7 (implementation details). Unrecognized messages and data should be identified and dispositioned by the receiving system in accordance with the pre-specified design requirements.	[[ ]]
33	Staff Position 1.7 (implementation details). Message format and protocol should be pre-determined.	Communication protocol specifications define the message structure, the message type, and the content of each message.
34	Staff Position 1.7 (implementation details). Every message should have the same message field structure and sequence, including message identification, status information, data bits, etc. in the same locations in every message.	Every message, as defined by the governing protocol specification, has the same message field structure including sequence, message ID, status information, data, and check sum.
35	Staff Position 1.7 (implementation details). Every datum should be included in every transmit cycle, whether it has changed since the previous transmission or not, to ensure deterministic system behavior.	Message format and protocol are pre-determined. Every message has the same message field structure and sequence (e.g., message identification, status information, data bits) in the same locations in every message. Every datum is included in every transmit cycle, whether it has changed due to the previous transmission or not.

	DI&C-ISG-04 Text/Guidance	CGS PRNM Conformance to DI&C-ISG-04
36	Staff Position 1.8. Data exchanged between redundant safety divisions or between safety and nonsafety divisions should be processed in a manner that does not adversely affect the safety function of the sending divisions, the receiving divisions, or any other independent divisions.	[[ ]] Note: Section 3.1 provides additional information (similar to GGNS-RAI 13) to address Staff Position 1.8.
37	Staff Position 1.9. Incoming message data should be stored in fixed predetermined locations in the shared memory and in the memory associated with the function processor. These memory locations should not be used for any other purpose. The memory locations should be allocated such that input data and output data are segregated from each other in separate memory devices or in separate pre-specified physical areas within a memory device.	[[ ]]

	DI&C-ISG-04 Text/Guidance	CGS PRNM Conformance to DI&C-ISG-04
38	Staff Position 1.10. Safety division software should be protected from alteration while the safety division is in operation.	[[ ]] Note: Sections 3.2 and 3.3 provide additional information (similar to GGNS-RAIs 16 and 17) to address Staff Position 1.10.
39	Staff Position 1.10 (implementation details). On-line changes to safety system software should be prevented by hardwired interlocks or by physical disconnection of maintenance and monitoring equipment. A workstation (e.g. engineer or programmer station) may alter addressable constants, setpoints, parameters, and other settings associated with a safety function only by way of the dual-processor / shared-memory scheme described in this guidance, or when the associated channel is inoperable. Such a workstation should be physically restricted from making changes in more than one division at a time. The restriction should be by means of physical cable disconnect, or by means of keylock switch that either physically opens the data transmission circuit or interrupts the connection by means of hardwired logic.	[[ ]]

	DI&C-ISG-04 Text/Guidance	CGS PRNM Conformance to DI&C-ISG-04
40.	Staff Position 1.10 (implementation details). "Hardwired logic" as used here refers to circuitry that physically interrupts the flow of information, such as an electronic AND gate circuit (that does not use software or firmware) with one input controlled by the hardware switch and the other connected to the information source: the information appears at the output of the gate only when the switch is in a position that applies a "TRUE" or "1" at the input to which it is connected. Provisions that rely on software to effect the disconnection are not acceptable. It is noted that software may be used in the safety system or in the workstation to accommodate the effects of the open circuit or for status logging or other purposes.	No software changes are allowed online; therefore, this switch is not used.
41.	Staff Position 1.11. Provisions for interdivisional communication should explicitly preclude the ability to send software instructions to a safety function processor unless all safety functions associated with that processor are either bypassed or otherwise not in service. The progress of a safety function processor through its instruction sequence should not be affected by any message from outside its division. For example, a received message should not be able to direct the processor to execute a subroutine or branch to a new instruction sequence.	[[ ]] Note: Section 3.4 provides additional information (similar to GGNS-RAI 12) to address Staff Position 1.11.

	DI&C-ISG-04 Text/Guidance	CGS PRNM Conformance to DI&C-ISG-04
42.	Staff Position 1.12. Communication faults should not adversely affect the performance of required safety functions in any way.	[[ ]] Note: Section 3.4 provides additional information (similar to GGNS-RAI 12) to address Staff Position 1.12.
43.	Staff Position 1.12 (Implementation details) Faults, including communication faults, originating in nonsafety equipment, do not constitute "single failures" as described in the single failure criterion of 10 CFR Part 50, Appendix A.	[[ ]]
44.	Staff Position 1.12 (Implementation details). Examples of credible communication faults include, but are not limited to, the following:	Title. Not a requirement.
45.	Staff Position 1.12 (Implementation details). Messages may be corrupted due to errors in communications processors, errors introduced in buffer interfaces, errors introduced in the transmission media, or from interference or electrical noise.	[[ ]]
46.	Staff Position 1.12 (Implementation details). Messages may be repeated at an incorrect point in time.	[[ ]]

	DI&C-ISG-04 Text/Guidance	CGS PRNM Conformance to DI&C-ISG-04
47	Staff Position 1.12 (Implementation details). Messages may be sent in the incorrect sequence.	[[ ]]
48	Staff Position 1.12 (Implementation details). Messages may be lost, which includes both failures to receive an uncorrupted message or to acknowledge receipt of a message.	[[ ]]
49	Staff Position 1.12 (Implementation details). Messages may be delayed beyond their permitted arrival time window for several reasons, including errors in the transmission medium, congested transmission lines, interference, or by delay in sending buffered messages.	[[ ]]
50	Staff Position 1.12 (Implementation details). Messages may be inserted into the communication medium from unexpected or unknown sources.	[[ ]]

	DI&C-ISG-04 Text/Guidance	CGS PRNM Conformance to DI&C-ISG-04
51	Staff Position 1.12 (Implementation details). Messages may be sent to the wrong destination, which could treat the message as a valid message.	[[ ]]
52	Staff Position 1.12 (Implementation details). Messages may be longer than the receiving buffer, resulting in buffer overflow and memory corruption.	[[ ]]
53	Staff Position 1.12 (Implementation details). Messages may contain data that is outside the expected range.	In this case the instrument declares the data invalid and the data is not used.
54	Staff Position 1.12 (Implementation details). Messages may appear valid, but data may be placed in incorrect locations within the message.	[[ ]]
55	Staff Position 1.12 (Implementation details). Messages may occur at a high rate that degrades or causes the system to fail (i.e., broadcast storm).	[[ ]]

	DI&C-ISG-04 Text/Guidance	CGS PRNM Conformance to DI&C-ISG-04
56	Staff Position 1.12 (Implementation details). Message headers or addresses may be corrupted.	The firmware rejects these messages.
57	Staff Position 1.13 Vital communications, such as the sharing of channel trip decisions for the purpose of voting, should include provisions for ensuring that received messages are correct and are correctly understood. Such communications should employ error-detecting or error-correcting coding along with means for dealing with corrupt, invalid, untimely or otherwise questionable data. The effectiveness of error detection/correction should be demonstrated in the design and proof testing of the associated codes, but once demonstrated is not subject to periodic testing. Error-correcting methods, if used, should be shown to always reconstruct the original message exactly or to designate the message as unrecoverable. None of this activity should affect the operation of the safety-function processor.	[[ ]] Note: Section 3.5 provides additional information (similar to GGNS-RAI 15) to address Staff Position 1.13.
58	Staff Position 1.14. Vital communications should be point-to-point by means of a dedicated medium (copper or optical cable). In this context, "point-to-point" means that the message is passed directly from the sending node to the receiving node without the involvement of equipment outside the division of the sending or receiving node. Implementation of other communication strategies should provide the same reliability and should be justified.	[[ ]]

	DI&C-ISG-04 Text/Guidance	CGS PRNM Conformance to DI&C-ISG-04
59	Staff Position 1.15. Communication for safety functions should communicate a fixed set of data (called the "state") at regular intervals, whether data in the set has changed or not.	[[ ]]
60	Staff Position 1.16. Network connectivity, liveness, and real-time properties essential to the safety application should be verified in the protocol. Liveness, in particular, is taken to mean that no connection to any network outside the division can cause an RPS/ESFAS communication protocol to stall, either deadlock or livelock. (Note: This is also required by the independence criteria of: (1) 10 CFR Part 50, Appendix A, General Design Criteria ("GDC") 24, which states, "interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired."; and (2) IEEE 603-1991 IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.) (Source: NUREG/CR-6082, 3.4.3)	[[ ]]

	DI&C-ISG-04 Text/Guidance	CGS PRNM Conformance to DI&C-ISG-04
61.	Staff Position 1.17. Pursuant to 10 CFR Part 50.49, the medium used in a vital communications channel should be qualified for the anticipated normal and post-accident environments. For example, some optical fibers and components may be subject to gradual degradation as a result of prolonged exposure to radiation or to heat. In addition, new digital systems may need susceptibility testing for EMI/RFI and power surges, if the environments are significant to the equipment being qualified.	[[ ]]
62.	Staff Position 1.18. Provisions for communications should be analyzed for hazards and performance deficits posed by unneeded functionality and complication.	[[ ]]

	DI&C-ISG-04 Text/Guidance	CGS PRNM Conformance to DI&C-ISG-04
63	Staff Position 1.19 If data rates exceed the capacity of a communications link or the ability of nodes to handle traffic, the system will suffer congestion. All links and nodes should have sufficient capacity to support all functions. The applicant should identify the true data rate, including overhead, to ensure that communication bandwidth is sufficient to ensure proper performance of all safety functions. Communications throughput thresholds and safety system sensitivity to communications throughput issues should be confirmed by testing.	[[ ]] Note: Section 3.6 provides additional information (similar to GGNS-RAI 18) to address Staff Position 1.19.
64	Staff Position 1.20. The safety system response time calculations should assume a data error rate that is greater than or equal to the design basis error rate and is supported by the error rate observed in design and qualification testing.	[[ ]] Note: Section 3.6 provides additional information (similar to GGNS-RAI 18) to address Staff Position 1.20.
65	**2.2. Command Prioritization**	Title. Not a requirement.

	DI&C-ISG-04 Text/Guidance	CGS PRNM Conformance to DI&C-ISG-04
66	**Scope:**	
67	This section presents guidance applicable to a prioritization device or software function block, hereinafter referred to simply as a "priority module."	Definition. Not a requirement.
68	A priority module receives device actuation commands from multiple safety and non-safety sources, and sends the command having highest priority on to the actuated device. The actuated device is a safety-related component such as a motor actuated valve, a pump motor, a solenoid operated valve, etc. The priority module must also be safety-related.	The APRM system does not use priority modules. Therefore, this section does not apply. The system is designed as a fail-safe (fail in a trip state). The actuation of the solenoid valves is performed by the reactor protection system (RPS).
69	**STAFF POSITION**	Title. Not a requirement.
70	Existing Diversity and Defense-in-Depth guidance indicates that diverse actuation signals should be applied to plant equipment control circuits downstream of the digital system to which they are diverse, in order to ensure that the diverse actuation will be unaffected by digital system failures and malfunctions. Accordingly the priority modules that combine the diverse actuation signals with the actuation signals generated by the digital system should not be executed in digital system software that may be subject to common-cause failures (CCF).	[[ ]] Note: Section 3.7 provides additional information (similar to GGNS-RAI 19) to address Staff Position 2.0.

	DI&C-ISG-04 Text/Guidance	CGS PRNM Conformance to DI&C-ISG-04
71	Software implementation of priority modules not associated with diverse actuation would result in the availability of two kinds of priority modules, one of which is suitable for diverse actuation and one type not suitable for diverse actuation. An applicant should demonstrate that adequate configuration control measures are in place to ensure that software-based priority modules that might be subject to CCF will not be used later for credited diversity, either deliberately or accidentally (for example, there is protection from design error and from maintenance / implementation error). This applies both to existing diversity provisions and to diversity provisions that might be credited later. The applicant should show how such provisions fit into the overall Appendix B quality program.	As discussed above, this requirement does not apply to PRNM. [[ ]]
72	Staff Position 2.1. A priority module is a safety related device or software function. A priority module must meet all of the 10 CFR Part 50, Appendix A and B requirements (design, qualification, quality, etc.) applicable to safety-related devices or software.	N/A for PRNM
73	Staff Position 2.2. Priority modules used for diverse actuation signals should be independent of the remainder of the digital system, and should function properly regardless of the state or condition of the digital system. If these recommendations are not satisfied, the applicant should show how the diverse actuation requirements are met.	N/A for PRNM

	DI&C-ISG-04 Text/Guidance	CGS PRNM Conformance to DI&C-ISG-04
74	Staff Position 2.3. Safety-related commands that direct a component to a safe state must always have the highest priority and must override all other commands. Commands that originate in a safety-related channel but which only cancel or enable cancellation of the effect of the safe-state command (that is, a consequence of a Common-Cause Failure in the primary system that erroneously forces the plant equipment to a state that is different from the designated "safe state."), and which do not directly support any safety function, have lower priority and may be overridden by other commands. In some cases, such as a containment isolation valve in an auxiliary feedwater line, there is no universal "safe state:" the valve must be open under some circumstances and closed under others.	[[ ]] Note: Section 3.8 provides additional information (similar to GGNS-RAI 14) to address Staff Position 2.3.

	DI&C-ISG-04 Text/Guidance	CGS PRNM Conformance to DI&C-ISG-04
75	Continuation of Staff position 2.3 description. The relative priority to be applied to commands from a diverse actuation system, for example, is not obvious in such a case. This is a system operation issue, and priorities should be assigned on the basis of considerations relating to plant system design or other criteria unrelated to the use of digital systems. This issue is outside the scope of this ISG. The reasoning behind the proposed priority ranking should be explained in detail. The reviewer should refer the proposed priority ranking and the explanation to appropriate systems experts for review.	N/A for PRNM
76	Staff Position 2.3. (implementation details). The priority module itself should be shown to apply the commands correctly in order of their priority rankings, and should meet all other applicable guidance. It should be shown that the unavailability or spurious operation of the actuated device is accounted for in, or bounded by, the plant safety analysis.	N/A for PRNM
77	Staff Position 2.4. A priority module may control one or more components. If a priority module controls more than one component, then all of these provisions apply to each of the actuated components.	N/A for PRNM
78	Staff Position 2.5. Communication isolation for each priority module should be as described in the guidance for interdivisional communications.	N/A for PRNM

	DI&C-ISG-04 Text/Guidance	CGS PRNM Conformance to DI&C-ISG-04
79	Staff Position 2.6. Software used in the design, testing, maintenance, etc. of a priority module is subject to all of the applicable guidance in Regulatory Guide 1.152, which endorses IEEE Standard 7-4.3.2-2003 (with comments). This includes software applicable to any programmable device used in support of the safety function of a prioritization module, such as programmable logic devices (PLDs), programmable gate arrays, or other such devices. Section 5.3.2 of IEEE 7-4.3.2-2003 is particularly applicable to this subject. Validation of design tools used for programming a priority module or a component of a priority module is not necessary if the device directly affected by those tools is 100% tested before being released for service. 100% testing means that every possible combination of inputs and every possible sequence of device states is tested, and all outputs are verified for every case. The testing should not involve the use of the design tool itself. Software-based prioritization must meet all requirements (quality requirements, V&V, documentation, etc.) applicable to safety-related software.	N/A for PRNM

	DI&C-ISG-04 Text/Guidance	CGS PRNM Conformance to DI&C-ISG-04
80	Staff Position 2.7. Any software program that is used in support of the safety function within a priority module is safety-related software. All requirements that apply to safety-related software also apply to prioritization module software. Nonvolatile memory (such as burned-in or reprogrammable gate arrays or random-access memory) should be changeable only through removal and replacement of the memory device. Design provisions should ensure that static memory and programmable logic cannot be altered while installed in the module. The contents and configuration of field programmable memory should be considered to be software, and should be developed, maintained, and controlled accordingly.	N/A for PRNM
81	Staff Position 2.8. To minimize the probability of failures due to common software, the priority module design should be fully tested (This refers to proof-of-design testing, not to individual testing of each module and not to surveillance testing.). If the tests are generated by any automatic test generation program then all the test sequences and test results should be manually verified. Testing should include the application of every possible combination of inputs and the evaluation of all of the outputs that result from each combination of inputs. If a module includes state-based logic (that is, if the response to a particular set of inputs depends upon past conditions), then all possible sequences of input sets should also be tested. If testing of all possible sequences of input sets is not considered practical by an applicant, then the applicant should identify the testing that is excluded and justify that exclusion.	N/A for PRNM

	DI&C-ISG-04 Text/Guidance	CGS PRNM Conformance to DI&C-ISG-04
82	Staff Position 2.9. Automatic testing within a priority module, whether initiated from within the module or triggered from outside, and including failure of automatic testing features, should not inhibit the safety function of the module in any way. Failure of automatic testing software could constitute common-cause failure if it were to result in the disabling of the module safety function.	N/A for PRNM
83	Continuation of Staff Position 2.9 description. The applicant should show that the testing planned or performed provides adequate assurance of proper operation under all conditions and sequences of conditions. Note that it is possible that logic devices within the priority module include unused inputs: assuming those inputs are forced by the module circuitry to a particular known state, those inputs can be excluded from the "all possible combinations" criterion. For example, a priority module may include logic executed in a gate array that has more inputs than are necessary. The unused inputs should be forced to either "TRUE" or "FALSE" and then can be ignored in the "all possible combinations" testing.	N/A for PRNM
84	Staff Position 2.10. The priority module must ensure that the completion of a protective action as required by IEEE Standard 603 is not interrupted by commands, conditions, or failures outside the module's own safety division.	N/A for PRNM
85	**2.3. Multidivisional Control And Display Stations**	Title. Not a requirement.

	DI&C-ISG-04 Text/Guidance	CGS PRNM Conformance to DI&C-ISG-04
86	**Scope:**	Title. Not a requirement.
	Staff Position 3.0. This section presents guidance concerning operator workstations used for the control of plant equipment in more than one safety division and for display of information from sources in more than one safety division. This guidance also applies to workstations that are used to program, modify, monitor, or maintain safety systems that are not in the same safety division as the workstation. Multidivisional control and display stations addressed in this guidance may themselves be safety-related or not safety-related, and they may include controls and displays for equipment in multiple safety divisions and for equipment that is not safety-related, provided they meet the conditions identified herein. Even though the use of multidivisional control and display stations is relatively new to the nuclear industry, the concepts to maintain the plant safety contained in this guidance is in line with the current NRC regulations.	
87	**GENERIC COMMENTS**	The PRNM does not have control stations, which can be used to operate equipment. The PRNM does not have equipment to monitor equipment in multiple divisions. An optional Operator Display Panel per division is installed in the MCR to provide the operator divisional status and information but has no control or maintenance functions. Therefore this section does not apply.
	This compliance matrix uses the term requirements and guidance synonymously. It is recognized that the ISG is guidance however for practicality, the sections of this ISG will be evaluated as requirements.	

3. Supplemental Information

The original wording of the GGNS RAIs has been modified to reflect the equipment, architecture, and documentation of the CGS PRNM system. These modifications are shown in blue text.

3.1. Staff Position 1.8 (GGNS-RAI 13)

Staff Position 1.8 of DI&C-ISG-04 states that "Data exchanged between redundant safety divisions or between safety and nonsafety divisions should be processed in a manner that does not adversely affect the safety function of the sending divisions, the receiving divisions, or any other independent divisions."

Describe in detail each of the following four (4) interfaces to satisfy the above criteria or to determine the proposed approach is an acceptable alternative:

i) Interface(s) between the RBM and the RMCS

ii) Interface(s) between the two-out-of-four voter and the RMCS

iii) Inter-divisional interfaces between RBMs

iv) Inter-divisional interfaces between two-out-of-four voters

For each interface describe:

a) whether it is an interface between non-safety and safety, or non-safety and non-safety;

b) how independence among safety-divisions is maintained through an explanation of the protocol, data and signal format, data flow, and isolation provided;

c) the evaluation of the interface to satisfy DI&C-ISG-04 and BTP 7-19 or the justification why the criteria does not apply;

d) the corresponding section(s) of the PRNMS LTR that describes the interface.

CGS PRNM Response

3.1.1 Interface(s) Between the RBM and RMCS

(a) Interface Classification

[[

]]

(b) Safety System Independence

Because this is a non-safety to non-safety related interface, the safety system independence requirement does not apply.

(c) DI&C-ISG-04 and BTP 7-19 Requirements

The criteria for DI&C-ISG-04 and Branch Technical Position (BTP) 7-19 do not apply for the RBM to RMCS interface because it is a non-safety to non-safety interface.

(d) PRNMS LTR Sections

[[

]]

3.1.2 Interface(s) Between the 2-Out-Of-4 Logic Module and the RMCS

(a) Interface Classification

[[

]]

[[ ]] the RMCS to the CGS PRNM.

(b) Safety System Independence

[[

]] Isolators are provided for the outputs between the 2-Out-Of-4 logic modules and RMCS, and therefore equipment failures will not affect the safety-related functions of other PRNM channels.

(c) DI&C-ISG-04 and BTP 7-19 Requirements

This interface meets the criteria of DI&C-ISG-04 as described in the response to Staff Position 1.8 provided in Section 2, CGS DI&C-ISG-04 Compliance Matrix. [[

]]

(d) PRNMS LTR Sections

[[

]]

3.1.3 Interdivisional Interfaces Between RBMs

The interdivisional interfaces identified in the original NRC request pertained to the use of Power Range Communication Interface (PCI) modules which provide certain functionality

similar to that provided by the RBMs used within the CGS PRNM, but also provide additional functionality not found in the RBMs – nor required for the CGS PRNM.

The additional functionality provided by the four PCI modules – each dedicated to a single APRM channel – required interdivisional interfaces between those PCIs.

As shown in Figure 1, there are no communication links between the two RBMs used in the CGS PRNM, and therefore the concerns related to the interdivisional interfaces between PCI modules are not applicable to the CGS PRNM.

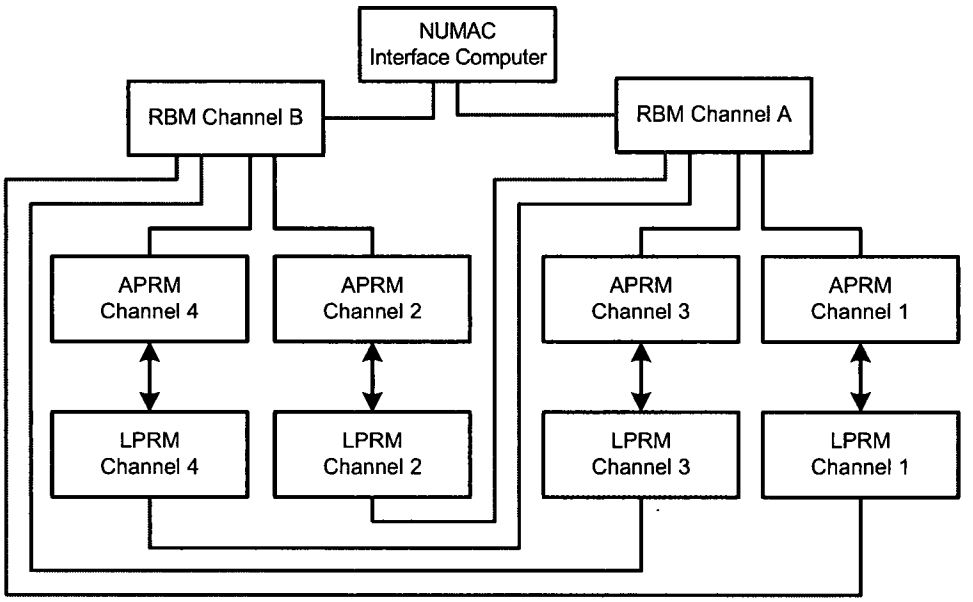

Figure 1 - RBM Communication Links

3.1.4 Interdivisional Interfaces Between 2-Out-Of-4 Logic Modules

(a) Interface Classification

[[

]] Therefore, this is a safety-to-safety interface among safety channels.

(b) Safety System Independence

[[

]]

(c) DI&C-ISG-04 and BTP 7-19 Requirements

[[ ]] Therefore, the criteria for DI&C-ISG-04 and BTP 7-19 do not apply for the interdivisional interfaces between the 2-Out-Of-4 logic modules.

[[

]] CGS DI&C-ISG-04 Compliance Matrix.

(d) PRNMS LTR Sections

[[

]]

References

1. GE Nuclear Energy, "Nuclear Measurement Analysis and Control Power Range Neutron Monitor (NUMAC PRNM) Retrofit Plus Option III Stability Trip Function," NEDC-32410P-A, October 1995.

[[

]]

Figure 2 – 2-Out-Of-4 Logic Module Interfaces

3.2. Staff Position 1.10 (GGNS-RAI 16)

Staff Position 1.10 of DI&C-ISG-04 governs communications of a safety division with maintenance and monitoring equipment.

Describe in detail the communications used in performance of maintenance and monitoring to completely address Staff Position 1.10 of DI&C-ISG-04, including the following to satisfy the above criteria or to determine the proposed approach is an acceptable alternative:

a) whether the dedicated division's local front panel is required to be used to confirm gain adjustments prior to use and without regard to the method used to provide gains to the APRM;

b) whether only one division's gains may be confirmed/accepted at a time;

c) whether the communication path that provides gains to the APRM via the NUMAC Interface Computer is connected and active at all times; and

d) whether the restriction to adjust only one division's gains at a time is by means of physical cable disconnect, or by means of keylock switch that either physically opens the data transmission circuit or interrupts the connection by means of hardwired logic (versus reliance upon a combination of firmware enable, password and/or reading keylock position, and administrative controls).

CGS PRNM Response

The PRNM system architecture does not allow software changes online. [[

]] This satisfies the DI&C-ISG-04 Staff Position 1.10 requirements that "Safety division software should be protected from alteration while the safety division is in operation. On-line changes to safety system software should be prevented by hardwired interlocks or by physical disconnection of maintenance and monitoring equipment."

[[

]]

Changes to parameters and setpoints, including the gains, in a given APRM channel can only be made from the front panel display of the master APRM instrument or LPRM instrument in that channel. [[

]]

Further discussion about the communication over the dedicated serial data link is below in the response to (c). This is an alternative to the DI&C-ISG-04 Staff Position 1.10 requirement that "A workstation (e.g. engineer or programmer station) may alter addressable constants, setpoints, parameters, and other settings associated with a safety function only by way of the dual processor / shared memory scheme described in this guidance, or when the associated channel is inoperable."

There is no common maintenance workstation that could be used to accept pending gains or alter any addressable constants, setpoints, parameters, or other settings in more than one channel at a time. This meets the DI&C-ISG-04 Staff Position 1.10 requirement that "Such a workstation should be physically restricted from making changes in more than one division at a time. The restriction should be by means of physical cable disconnect, or by means of keylock switch that either physically opens the data transmission circuit or interrupts the connection by means of hardwired logic."

The two types of gains specifically discussed in this response are APRM gain (based on core thermal power) and LPRM detector gains (based on LPRM gain adjustment factors). The pending APRM gain and pending LPRM detector gain adjustment data can be downloaded from the plant process computer, but they must still be accepted at the master APRM instrument or LPRM instrument front panel display. The pending APRM gain and the pending LPRM gains for the LPRM detectors processed at the master APRM instrument are accepted at the master APRM instrument front panel display, not at the LPRM instrument front panel display. The pending gains for LPRM detectors processed at the LPRM instrument are accepted at the LPRM instrument front panel display, not at the master APRM instrument front panel display. The high level communication path for pending gains downloaded from the plant process computer is shown below in Figure 3.

[[

]]

Figure 3 Communication Path for Pending Gains

[[

]]

Additional information about changing APRM gain and LRPM detector gains is discussed below.

a) As stated above, the front panel display of the master APRM instrument or LPRM instrument within an APRM channel must be used to confirm the pending APRM gain adjustment and pending LPRM detector gain adjustments for that APRM channel, regardless of the method used to provide the pending gains to the APRM channel.

   [[

]]

b) Each master APRM instrument and LPRM instrument in each of the four APRM channels has its own front panel display. As stated above, the pending gains for a given APRM channel can only be accepted from the front panel display of the master APRM instrument or LPRM instrument in that APRM channel.

c) The communication path that provides pending gains to the master APRM instrument and LPRM instrument from the NIC is connected and active at all times. The communication path has been analyzed and demonstrated not to effect the APRM's ability to perform its safety function, as discussed below.

[[

]]

d) As stated above, there is no common maintenance workstation that could be used to accept pending gains in more than one APRM channel at a time. Therefore the requirement to physically restrict connection of such a workstation to only one APRM channel at a time as described in DI&C-ISG-04 Staff Position 1.10 is met. A combination of security features in

conjunction with administrative controls are used to restrict access to the setup screens that allow gain adjustments to be made, as described above in the discussion about the different security levels.

References

1. GE Nuclear Energy, "Nuclear Measurement Analysis and Control Power Range Neutron Monitor (NUMAC PRNM) Retrofit Plus Option III Stability Trip Function," NEDC-32410P-A, October 1995.
2. GEH NUMAC PRNM Requirements Specification, 24A5221.
3. GEH PRNMS FDDI Protocol Specification, 24A5244.
4. GEH APRM Internal Communication Protocol Performance Specification, 26A7960.
5. GEH APRM Functional Software Design Specification, 26A6774.

3.3. Staff Position 1.10 (GGNS-RAI 17)

With respect to maintenance and monitoring, describe the administrative controls using terminology consistent with the LTR and in full consideration of the response provided in 3.2, Staff Position 1.10 (GGNS-RAI 16) above sufficiently to address:

a) Whether the activities associated with use of the OPERATE-SET mode are achieved at the local channel's front panel;

b) How the OPERATE-SET mode is entered; and

c) To explicitly map the description to the three levels of security that are identified in the LTR paragraph 5.3.13.

The following further clarifies the rationale for this RAI but does not include additional information requests. The response to a previous request did not use the same terminology as the LTR and is difficult to correlate with the response provided for Staff Position 1.10 of DI&C-ISG-04 or key switch position/features that may be built into a NUMAC chassis.

CGS PRNM Response

The following is a description of the administrative controls, using terminology consistent with Section 5.3.13 of the LTR (NEDC-32410P-A, Reference 1), to address items a, b and c above:

[[

]]

The key for the keylock switch and password will be controlled by Operations in accordance with plant procedures.

References

1. GE Nuclear Energy, "Nuclear Measurement Analysis and Control Power Range Neutron Monitor (NUMAC PRNM) Retrofit Plus Option III Stability Trip Function," NEDC-32410P-A, October 1995.
2. NUMAC PRNM Requirements Specification, 24A5221TC.
3. APRM User's Manual, 26A7865.

3.4. Staff Positions 1.11 and 1.12 (GGNS-RAI 12)

Staff Position 1.11 of DI&C-ISG-04 states, in part, that "The progress of a safety function processor through its instruction sequence should not be affected by a message from outside its division." Staff Position 1.12 of DI&C-ISG-04 states, in part, that "Communication faults should not adversely affect the performance of required safety functions in any way."

Describe in detail how firmware within the OPRM/APRM chassis, which is considered safety-related ensures the integrity of all data processed within the OPRM/APRM (e.g. valid message formats and ranges) to satisfy the above criteria or to determine the proposed approach is an acceptable alternative.

The information provided in the ISG-04 Compliance Matrix has not described data flows or the communication protocol by which non-safety system data is provided to each redundant OPRM/APRM channel for processing. No description of the processing is provided to identify whether the data directly affects the safety processor for either safety function or support software, and whether this data processing is limited to a channel in INOP or BYPASS as determined by the safety processor. There is no need to address information previously described for hardware-based integrity checks associated with the communication protocol and data buffering that have not changed since the PRNMS LTR.

CGS PRNM Response

The following response details the alternative approach of the APRM to Staff Position 1.11 and explains how the APRM satisfies the criteria of Staff Position 1.12.

[[

]]

Message Title	Usage Description
[[	
	]]

[[

]]

No communication fault will adversely affect the performance of required safety functions and the APRM meets the criteria of Staff Position 1.12.

3.5. Staff Position 1.13 (GGNS-RAI 15)

DI&C-ISG-04 Position 1.13 states for communications that are needed to support a safety function, the effectiveness of error detection/correction should not affect the operation of the safety-function. Furthermore DI&C-ISG-04 Position 1.19 states that communications throughput thresholds and safety system sensitivity to communications throughput issues should be confirmed by testing.

Describe in detail the methods used to test that each safety processor within PRNMS upgrade cannot be adversely influenced by the non-safety or inter-divisional communications activities.

[Note: The original RAI identified a list of interfaces specific to the architecture and equipment of the GGNS PRNM, and the information provided in the response was specific to that list. Rather than addressing the list of comparable CGS PRNM interfaces, the response below identifies the documentation generated for the CGS PRNM project which provide the information and analysis which address Staff Positions 1.13 and 1.19.]

CGS PRNM Response

For background information, detailed descriptions related to CGS PRNM, safety-to-safety, safety-to-nonsafety, and nonsafety-to-nonsafety communication interfaces can be found in the NEDC-33696P (Reference 1).

Section 3.4, Staff Positions 1.11 and 1.12 (GGNS-RAI 12) describes both the validation and error checking within discussion related to the processing of FDDI messages.

NEDC-33690P (Reference 2) identifies the data related to error rates, message intervals, communication throughput capacity, and delay times utilized by the analysis.

As noted within the evaluation of DI&C-ISG-04 Staff Positions 1.19 and 1.120 provided in Reference 2: the CGS PRNM V&V test plan include steps to address capacity usage during nominal and increased usage operation, and notes that "data error rates will be supported by testing a similar PRNM system for GGNS during integration testing."

References

1. GE Hitachi Nuclear Energy, "Columbia Generating Station Power Range Neutron Monitoring System Architecture & Theory of Operations Report, NEDC-33696P, Revision 0, November 2011.
2. GE Hitachi Nuclear Energy, "Columbia Generating Station Power Range Neutron Monitoring System Response Time Analysis Report," NEDC-33690P, Revision 0, November 2011.

3.6. Staff Positions 1.19 and 1.20 (GGNS-RAI 18)

Staff Positions 1.19 and 1.20 of DI&C-ISG-04 address the potential impact of data throughput and data error rates on worst-case response time.

Describe in detail the testing performed to ensure proper performance of all safety functions to satisfy the above criteria or to determine the proposed approach is an acceptable alternative.

CGS PRNM Response

As noted above in Section 3.5, NEDC-33690P (Reference 1) documents an evaluation which demonstrates that the criteria of DI&C-ISG-04 Staff Positions 1.19 and 1.120 have been satisfied.

References

1. GE Hitachi Nuclear Energy, "Columbia Generating Station Power Range Neutron Monitoring System Response Time Analysis Report," NEDC-33690P, Revision 0, November 2011.

3.7. Staff Position 2.0 (GGNS-RAI 19)

Staff Position on Command Prioritization of DI&C-ISG-04 could apply to the 2-out-of-4 voter design if the same 2-out-of-4 voter (or a common design) is used to process any of the following in addition to the PRNMS trips:

a) the diverse actuation signals in addition to those generated by the PRNMS which are identified in Table 2-1, Sensor Diversity for Initiating Events, of Reference 1 below; or

b) the Manual Trips signal;

[Note: A reference to the DSS-CD function in the original RAI is not applicable to the CGS PRNM.]

Describe the plant's intended use of the PRNMS 2-out-of-4 voter design to satisfy the above criteria or to determine the proposed approach is an acceptable alternative and include justification, as applicable, that evaluates criteria within DI&C-ISG-02 and BTP 7-19.

CGS PRNM Response

As noted in the DI&C-ISG-04 compliance matrix, Item 68 [[

]]

The following addresses the two items above:

a) As noted in Section 2.3 of Reference 1: "The PRNM System replaces a single-sensor input to the Reactor Protection System (RPS), but does not change or alter the plant-level diversity between RPS and other plant systems. Other sensor inputs within RPS (e.g., reactor dome pressure) are diverse from the PRNM System since these other sensor inputs do not utilize the NUMAC platform. Therefore, they are not subject to the same common-cause failures."

[[

]]

References

1. GE Hitachi Nuclear Energy, "Columbia Generating Station Power Range Neutron Monitoring System Diversity and Defense-in-Depth (D3) Analysis," NEDC-33694P, Revision 1, January 2012.

3.8. Staff Position 2.3 (GGNS-RAI 14)

For the inter-divisional communications interface between 2-out-of-4 voter channels, further describe in detail:

a) any function that the programmed PLD performs in support of these communications;

b) If this inter-divisional communications exists and a common programmed PLD is involved in all four divisions, then include an additional evaluation of this interface to satisfy BTP 7-19 or to determine that the proposed approach is an acceptable alternative. Otherwise the detail may justify why the criteria does not apply.

The figure which had been previously submitted did not identify direct 2-out-of-4 voter inter-divisional communications; however, the previously submitted DI&C-ISG-04 matrix response to Staff Position 2.3 stated that "The voter using hardware logic sends a fiber-optic signal to the other divisions." Also, the previously submitted figure showed "SELF TEST DATA & BYPASS STATUS DATA" from each 2-out-of-4 voter to its divisions APRMs, where the APRM could then feedback its status to all four voters. However, the replacement figure neither depicts this signal flow nor other inter-divisional communications between 2-out-of-4 voters. Therefore, it is unclear whether 1) the "SELF TEST DATA & BYPASS STATUS DATA" interface still exists or 2) inter-divisional communications between 2-out-of-4 voters exist.

CGS PRNM Response

3.8.1. Functions Performed By Programmed PLD

This response follows the convention of other responses in that the term division is used only with respect to the RPS. The term channel is used in all other cases.

For the inter-channel communications interface between 2-Out-Of-4 Logic Modules (voter channels), PLD U11 supports the Channel Bypass signal communications that are unidirectional from each 2-Out-Of-4 Logic Module to all of the other 2-Out-Of-4 Logic Modules. These are the only inter-channel communication interfaces between 2-Out-Of-4 Logic Modules. Refer to Figure 2 and Figure 4.

The inter-channel interfaces receive simple pulse stream signals indicating the status of the Bypass Switch. With the system functioning normally, either no channels or one channel can be bypassed, and therefore there will be at most one pulse stream signal.

[[

]]

3.8.2. Interdivisional Communications

[[

]]

[[	
	]]

In summary, a CCF in U11 such that a channel is incorrectly bypassed does not prevent trips. A CCF in U11 that results in multiple channels bypassed forces U21 to ignore bypasses. A CCF of U21 that causes multiple channels to be bypassed is detected by the APRM. It is concluded that failures related to the bypass signal processing either do not prevent trips or are detectable by the APRM.

[[

]]

Figure 4 - Inter-Channel Communication

[[

]]

Figure 5 - 2-Out-Of-4 Logic Card

Enclosure 2

CGS PRNMS Hardware, Software, and Software Development Changes

The information provided in this enclosure has been extracted from the previously submitted G02-10-099, "Columbia Generating Station, Docket No. 50-397 Response to Request for Supplemental Information for Completion of Acceptance Review for PRNM/ARTS/MELLLA System Upgrade," dated July 30, 2010 (ML102360357).

The portions of the response to RSI #1 which address ISG-06 Section D.8.2 was provided within the following parts:

- Part 1: NUMAC PRNM Platform Hardware Changes
- Part 2: NUMAC PRNM Platform Software Changes
- Part 3: NUMAC PRNM Platform Software Development Process Changes
- Tables of specific changes

These sections have been extracted and are provided within this enclosure.

Table of Contents

1. Part 1: NUMAC PRNM Platform Hardware Changes

The first PRNM system installed in the United States (US) was installed at Hatch in 1997. The PRNM platform at Hatch is identical to the platform described in PRNM LTR (NEDC-32410P-A), and therefore provides a basis for comparison to the platform that was originally reviewed and approved by the NRC. Tables 1-1, 1-2, and 1-3 show the differences in the NUMAC platform between the initial US application at Hatch in 1997 and the CGS PRNM application by comparing the part numbers of the hardware modules used in the Hatch application to the part numbers of the hardware modules used in the CGS application. Table 1-4 summarizes all the changes to the hardware modules by parts list revision since the initial US application at Hatch. Regardless of any hardware changes that have occurred since the original application, if the part number used for CGS is the same part number that was used for Hatch, then the part is fully interchangeable with respect to form, fit and function in accordance with GEH engineering operating procedures. The following paragraphs provide details of the significant hardware platform changes.

APRM Chassis Subassembly

[[

]]

GEDAC Communication/Memory Module

[[

]]

Relay Logic Card

[[

]]

2. Part 2: NUMAC PRNM Platform Software Changes

Table 1-5 identifies changes made to the safety-related generic APRM/OPRM firmware since the original design up to and including changes made for the CGS PRNM. The table lists the files containing revised firmware and a description of the changes. This table does not include changes made to the data files that are changed for each new plant application. These changes have been made in accordance with the NUMAC V&V process and the NUMAC configuration management process that were previously reviewed and approved by the NRC, as stated in Section 3.2 of the safety evaluation report (SER) in NEDC-32410P-A. The following is a synopsis of the APRM/OPRM software evolution process:

Design Inputs

[[

]]

Firmware Control

[[

]]

Firmware History

[[

]]

Firmware Testing

[[

]]

3. Part 3: NUMAC PRNM Platform Software Development Process Changes

[[

]] Section 3.2 of the SER in NEDC-32410P-A states that the standard NUMAC software development process defined by these plans and implemented for PRNM has been reviewed and accepted by the NRC. Consistent with the commitment that was made by GEH to the NRC as documented in Section 3.2 of the SER in NEDC-32410P-A, the NUMAC software development plans were issued as formally controlled corporate documents. Since the NRC first reviewed and approved the NUMAC software development plans, several changes have been made to these documents. These document changes were made in accordance with GEH procedures and in accordance with the required engineering and quality assurance reviews as was committed to the NRC at the time NEDC-32410P-A and these NUMAC software development plans were first reviewed and approved. The changes that have been made to these documents do not in any way alter the fundamental software life cycle process that was originally reviewed and approved by the NRC. Table 1-6 summarizes the revision history of the NUMAC software plans since they were first reviewed and approved by the NRC. Table 1-7 shows the correlation of the NUMAC design process to the requirements of BTP 7-14 Revision 5.

NUMAC Software Plans Revision History

[[

]]

BTP 7-14 Compliance

The primary NRC guideline available at the time the NUMAC design processes were developed was NRC RG 1.152 Revision 0 (1985), primarily endorsing ANSI/IEEE 7-4.3.2-1982. IEEE 7-4.3.2-1993 was issued prior to completion of the original PRNM design, but was not

endorsed by the NRC until 1996 (via RG 1.152 Revision 1). Evaluation of the NUMAC design process against both of those guides is included in NEDC-32410P-A, Appendix A. In addition, NEDC-32410P-A, Supplement 1, Appendix A, includes an evaluation of the process to ANSI NQA2, Part 2.7. A general description of the design process applied to the NUMAC PRNM is included in NEDC-32410P-A, Chapter 9. Finally, Appendix C in NEDC-32410P-A includes a comparison of the NUMAC PRNM equipment with NUMAC equipment previously designed and reviewed by the NRC.

Since the original PRNM design and NRC review of the NUMAC PRNM LTR, the NRC has issued BTP 7-14, Revision 5. This BTP and most of the NRC RGs listed therein were not issued at the time of the original design of the NUMAC PRNM equipment. BTP 7-14 guidance is intended to address complete digital systems in a plant, including full Reactor Trip Systems and Engineered Safety Features Systems. [[

]] Extensive field experience of NUMAC equipment, including PRNM, demonstrates that the design process applied for the NUMAC equipment, including PRNM, provides a fully adequate digital design for the NUMAC applications.

4. CGS PRNM Hardware Changes

4.1. Table 1-1. NUMAC Platform Changes – APRM Chassis

Module	Part Number Used for Hatch APRM (1997)	Part Number Used for CGS APRM (2010)
[[		
		]]

* [[

]]

4.2. Table 1-2. NUMAC Platform Changes – RBM Chassis

Module	Part Number Used for Hatch RBM (1997)	Part Number Used for CGS RBM (2010)
[[		
		]]

* [[

]]

4.3. Table 1-3. NUMAC Platform Changes – Two-Out-Of-Four Logic Module

Module	Part Number Used for Hatch 2-Out-Of-4 Logic Module (1997)	Part Number Used for CGS 2-Out-Of-4 Logic Module (2010)
[[		
		]]

* [[

]]

4.4. Table 1-4. Changes to Hardware Modules by Parts List Revision

Module	Part Number	Parts List Rev	Date	Description
[[				

Module	Part Number	Parts List Rev	Date	Description

Module	Part Number	Parts List Rev	Date	Description

Module	Part Number	Parts List Rev	Date	Description

Module	Part Number	Parts List Rev	Date	Description

Module	Part Number	Parts List Rev	Date	Description

Module	Part Number	Parts List Rev	Date	Description

Module	Part Number	Parts List Rev	Date	Description

Module	Part Number	Parts List Rev	Date	Description

Module	Part Number	Parts List Rev	Date	Description
				]]

5. CGS PRNM Firmware Changes

5.1 Table 1-5. NUMAC APRM/OPRM Firmware Changes

File	Description of Change	File Date
[[		

File	Description of Change	File Date

File	Description of Change	File Date

File	Description of Change	File Date

File	Description of Change	File Date

File	Description of Change	File Date

File	Description of Change	File Date

File	Description of Change	File Date
		]]

6. NUMAC Software Plans Revision History

6.1 Table 1-6. Revision History of NUMAC Software Plans

[[		

		]]