U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Non-Proprietary Version

RR901-001-03-NP,
Comment Descriptions to
Draft SE for Topical Report of HFC-6000, Rev. A
And Attachment of Draft SE with comments

DOOSAN

HF Controls

HF Controls

Comments to Draft SE for HFC-6000 System

RR901-001-03-NP Rev. A

Effective Date: 3-11-11

Prepared By: Ivan Chow

Reviewed By: Ed Herchenrader

Approved By: Ivan Chow

Revision History

Date	Revision	Preparer	Changes
3/11/11	A	I. Chow	Initial Revision

TABLE OF CONTENTS

Comments to Draft SE for HFC-6000 System

1.0 Introduction

This document contains the comments to the draft SE for HFC-6000 system received on 2-15-2011. Section 2.0 lists the comments.

2.0 Listing of the comments

No.	Location	Suggested Change	Type of Change	Justifications
1	p.6 Figure 1	The red dashed-line box should extend to cover the other node and the safety C-Link in the figure. See comments in the document.	Content	Safety C-Link communication is part of the review scope. See reference 1 of the draft SE and RAI #122 response.
2	p.6 line 21	Remove "one node of"	Content	Same justification as in comment no. 1
3	p.7 lines 13-19	Remove "While the network interface for the HFC-6000 controller is an integral platform nodes, the fiber optic network medium, including the fiber optic transmitters that provide electrical-to-optical coupling, are not within the scope of the platform. Also, ". Line 16, make "the gateway" become "The gateway". Lines 18-19, remove "or other systems, either safety-related or nonsafety-related,".	Content	Same reason as change no. 1. Plus HFC-ILR06 is part of the review scope. See table 1 of the draft SE.
4	p.18 line 11	add "and a controller reset" after "manual switch selection"	Content	Incorrect Information
5	p.20 line 5	"16-bit" should be changed to "12-bit"	Content	Incorrect Information
6	p.21 line 24	"twelve" should be "eleven"	Content	Incorrect Information
7	p.22 line 31	"DC33" should be changed to "DC34"	Typo	Incorrect Information
8	p.22 line 36	"DC33" should be changed to "DC34"	Typo	Incorrect Information
9	p.24 line 5	"Each AO channel consists" should be changed to "The AO circuitry is composed"	Content	For clarity.
10	p.28 line 7	It should be "PBUSIF" instead of "PBSUIF"	Typo	Incorrect Information

Comments to Draft SE for HFC-6000 System

No.	Location	Suggested Change	Type of Change	Justifications
11	p.52 line 4	It should be "CGD" instead of "CDG"	Typo	Incorrect Information
12	p.57 line 2	It should be "3.2.2.8" instead of "3.8"	Typo	Incorrect Information
13	p.61 line 29	Remove "Thus, the SInstP is an ASAI."	Content	All BTP 7-14 review plans apply to application.
14	p.106 lines 1-5	Paragraph lines 1 to 5 should be removed.	Content	Same justification as change no.1
15	p.121 lines 31-34	Remove "Although not in the scope of this evaluation" and insert "In addition" instead.	Content	Same justifications as change no.1 C-Link among intra-divisional communication is within scope.
16	p.187 item 5	Remove this open item	Content	Vague. Does not specify which "key performances" are not satisfied. Since HFC is committed to retest in accordance with TR 107330, this item is irrelevant.
17	p.187 items 6,7,8	They should be combined into 1 open item.	Content	Not logical. They are all related to EMC qualification. Splitting that into 3 open items make it like they can be independently passed without the others. However, in reality, EMC qualification CANNOT be passed with just one of these items get passed.
18	p.188 items 3,4	Combine this item 3 with item 4 by specifying "safety-related system project" in item 3.	Content	Item 3 covers item 4. The only difference between these two items is the "safety-related system project" in item 4, everything else is the same.
19	p.188 item 5	Remove this item. After item 3 and 4 combined, item 5 is automatically required by BTP 7-14.	Content	Redundant.
20	p.188 item 7	Remove this item.	Content	Redundant. It is covered by item 8.

Comments to Draft SE for HFC-6000 System

No.	Location	Suggested Change	Type of Change	Justifications
21	p.188 item 8	Add "Otherwise, the licensee must demonstrate the application using HFC-6000 platform qualifies plant-specific safety conditions.	Content	For clarity. With this statement, many of the plant-specific items can be eliminated.
22	p.188-p.189 items 9, 11, 13, 14	Remove these items.	Content	Redundant. Item 8 covers these 3 items. There are no ways that item 8 is satisfied while these 4 items cannot be satisfied.
23	p.190 items 19,25	Remove these items.	Content	Redundant. It is known that the TR of HFC-6000 does not cover any applications. No need to put application specific action items in the plant-specific action item list. It is like requiring a user using an operation system without a word processor to make sure run spell check at the time they use a word processor. Redundant and not meaningful.
24	p.190 item 23	Remove this item.	Content	Item 6 covers that.
25	p.191 items 28,29,30	Remove these items.	Content	It has nothing to do with HFC-6000 platform. Again, these are application specific and there are no applications specified in the TR.

3.0 Attachments

Draft SE for HFC-6000 with comments.

Legend for the marking of the comments:

1. Texts enclosed by a red box are to be removed.

   Example: one node of

2. Yellow text boxes are descriptions for the comments and not actual texts to be put into the document.

   Example: Combine these items.

3. Green text boxes are texts to be inserted to the documents.

   Example: PBUSIF

4. Texts enclosed by a green box are to be combined.

   Example:

   3. The licensee must demonstrate that execution of the HFC software QA program, with its constituent life cycle processes, plans, and procedures, for the planning, design, implementation, testing, and installation of application software, along with the introduction of any new functionality within the operating software (i.e., new software), complies with the regulatory requirements of Appendix B to 10 CFR Part 50 and is equivalent to industry standards and practices endorsed by the NRC, as referenced in SRP BTP 7-14 (see Section 2.1 of this SE).

   4. For a specific safety-related system project, the licensee is responsible for assuring that life cycle planning documentation for new software (e.g., application software) development under the HFC software QA program complies with the regulatory requirements of Appendix B to 10 CFR 50 and satisfies equivalent guidance to that provided by industry standards and practices endorsed by the NRC, as referenced in SRP BTP 7-14 (see Section 3.2.2 of this SE).

5. Red arrows are for locations of the comments or insertion texts. →

DRAFT SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

HFC-6000 SAFETY SYSTEM

DOOSAN HF CONTROLS CORPORATION

PROJECT NO. 731

1.0 INTRODUCTION AND BACKGROUND

By letter dated March 5, 2008 (Reference 1), as supplemented by letters dated November 15, 2007 (Reference 2), January 16, 2009 (Reference 3), May 29, 2009 (Reference 4), June 12, 2009 (Reference 5), July 20, 2009 (Reference 6), February 19, 2010 (Reference 7), March 12, 2010 (Reference 8), March 19, 2010 (Reference 9), May 6, 2010 (Reference 10), and June 18, 2010 (Reference 11), Doosan HF Controls Corporation (HFC) requested U.S. Nuclear Regulatory Commission (NRC) approval for the "HFC-6000 Safety System" topical report (TR), document number PP901-000-01, Revision C (Reference 12). The supplemental documents transmitted by letters dated November 15, 2007, and January 16, 2009, through May 6, 2010, provided additional information that clarified and supported the technical claims documented in the TR and did not expand or change the scope of the TR.

The TR was accepted for review by letter dated September 16, 2008 (Reference 13). The acceptance letter identified HFC commitments to supply supplemental documents based on discussions at a meeting between HFC and NRC staff in Rockville, Maryland, on August 19, 2008. These documents provide additional information to support the review of the design details and qualification of the HFC-6000 platform and were transmitted by letter dated January 16, 2009 (Reference 14). Revised and supporting documents were subsequently submitted under supplemental letters (References 4 through 11).

The TR provides a description of the HFC-6000 nuclear safety-related instrumentation and control (I&C) platform. The HFC-6000 platform is intended to serve as a qualified generic digital I&C platform that is suitable for the use in safety-related applications at U.S. nuclear power plants. Typical applications to be supported by the HFC-6000 platform include:

- reactor protection system (RPS),
- engineered safety features actuation system (ESFAS) functions,
- post accident monitoring system (PAMS) and safety parameter display system SPDS), and
- nuclear steam supply system (NSSS) and balance of plant (BOP) safety control systems and related functions.

Enclosure

The TR describes the hardware and software components of the HFC-6000 platform and addresses the design and qualification techniques used to ensure its quality and assess its reliability. Specifically, the report includes hardware and software design descriptions as well as a discussion of design characteristics relevant to selected safety criteria. Hardware qualification by type testing is addressed, in addition to the verification and validation of software quality through commercial grade dedication of predeveloped software for the platform.

The NRC staff conducted audits at the HFC facility in Carrolton, Texas, during the weeks of October 6-9, 2009, and December 16-18, 2009 (References 15 and 16). The purpose of the audits was to inspect HFC procedures and processes that are referenced in the TR and audit documented products of commercial grade dedication activities. During the site visits, thread audits were performed, the hardware configuration of the HFC-6000 qualification test specimen was observed, and performance characteristics and functional capabilities of the platform were demonstrated.

2.0 REGULATORY EVALUATION

The purpose of this safety evaluation (SE) of the TR is to evaluate whether the HFC-6000 platform is suitable for use in safety-related applications. Thus, the review of the TR and supporting technical documents is intended to determine whether sufficient evidence is presented to enable a determination with reasonable assurance that subsequent applications based on the platform can comply with the applicable regulations to ensure that the public health and safety will be protected. This review and associated audit activities are not intended to completely evaluate all aspects of the design and implementation of any specific safety-related application and full compliance with relevant regulations will need to be evaluated on a plant-specific basis. However, the review scope is sufficient to allow the reviewer to reach the conclusion of reasonable assurance within the platform-level context.

2.1 Scope of HFC-6000 Platform

As described in the TR, the HFC-6000 is a computer-based platform composed of programmable logic controller (PLC) modules providing control, input and output (I/O), and communication functionality. The base platform consists of equipment chassis housing dual-redundant controllers, I/O modules, and power supplies. For safety-related use, internal redundancy is provided as part of the base platform architecture through redundant controllers, redundant network connections, redundant bus links to I/O modules, and redundant power supplies. The redundant controllers operate in a primary/secondary configuration with a failover mechanism provided to enable transfer of primary control status to the secondary or "hot standby" controller.

The HFC-6000 controller and I/O modules are microprocessor-based printed circuit boards (PCBs) with operating (or system) software installed in firmware. Application software is installed in firmware and/or Flash memory to be executed by the HFC-6000 controller. Communication functions to support the transmission of data between the controller and I/O modules and the broadcast of status information and data among instances (or nodes) of the platform on an internal network are provided by dedicated processors within each controller module. Table 1 identifies the particular modules and components within the scope of the HFC-6000 platform (Reference 17). Each module is identified uniquely by a module number and name coupled with the corresponding part number (P/N) and revision. The firmware for a module is identified by a unique software part number. For the HFC-SBC06 controller module, part numbers identify the firmware for each of the three microprocessors resident on the PCB as well as the supporting board-level chipset, which is implemented using complex programmable logic devices (CPLDs). The hardware and software components identified in this table establish the platform scope covered by the TR under review. If this TR is referenced in plant licensing documentation, it is an application-specific action item (ASAI) to clearly identify any modification or addition to the base HFC-6000 platform as it is employed in a specific application that is subject to regulatory review (see Section 5.0 of this SE).

The HFC-6000 platform is based on the HFC product lines AFS-1000 and ECS-1200. The HFC-6000 hardware is derived from the ECS-1200 hardware, with the primary differences associated with changes in form factor to accommodate a 19-inch rack and repackage current ECS-1200 components on the HFC-6000 controller board (Reference 17). The operating software for the HFC-6000 platform is predeveloped software (PDS) from the heritage product lines. Operating software is the basic platform software that provides the system services and execution environment to support implementation of a specific application. The TR describes the commercial grade dedication (CGD) and qualification of the software and hardware for the HFC-6000 platform to facilitate use in safety-related applications at nuclear power plants.

Software supported by the HFC-6000 platform consists of operating software and application software. The principal focus for evaluation of HFC-6000 software involves the CGD of the PDS. The operating software for the HFC-6000 platform consists of a generic operating system, a task scheduler, a library of analog control algorithms, network and bus communications protocol software, and the software management mechanism for redundancy and failover. Self-test and diagnostic functionality is embedded in the operating software for each module. Application software is based on configuration of computational functions and function blocks supplied as part of the operating software. However, the TR does not address any particular safety-related implementation of the HFC-6000 platform so application software, which is necessarily specific to a plant system, is not within the scope of this SE.

Although the software life cycle processes and associated plans that are established by HFC are described in the TR, the implementation of that quality assurance (QA) program for safety-related application software is not presented. HFC has confirmed that it is not seeking approval of the application software development process or associated plans and procedures through this TR (Reference 14). Thus, the review of the HFC software QA program is limited to assessment of the process, plans, and procedures as they relate maintaining the commercially dedicated PDS. In the context of this evaluation, maintenance is defined as the process of modifying a software design output to repair nonconforming items or to implement preplanned actions necessary to maintain performance. Other modifications to the PDS to enhance functionality or adapt to a specific application are not considered to be maintenance and are addressed in connection with the implementation of the HFC software QA program for new software development, which is not within the scope of this review. Consequently, execution of the HFC software QA program, with its constituent life cycle processes, plans, and procedures, for the planning, design, implementation, testing, and installation of application software, along with any new functionality within the operating software (i.e., new software), is an ASAI and is subject to plant-specific review (see Section 5.2 of this SE).

Table 1 – List of Modules and Components for the HFC-6000 Platform

Module	P/N	Rev	Firmware/CPLD P/N
600W 24V Power Supply	9044524Q		
600W 48V Power Supply	9044525Q		
HFC-BPC01-19 Controller Backplane	40040701	E	
HFC-BPE01-19 Expansion Backplane	40041201	A	
HFC-SBC06 Controller	40041701	P	SC Firmware: 9120905-13
			SAP Firmware: 9120906-12
			SEP Firmware: 9120907-12
			SBC6_CHSEL CPLD: 9093075-11
			SBC6_386C CPLD: 9093074-12
			SBC6_SHARB CPLD: 9093076-11
			PBUSIF CPLD: 9093073-11
HFC-DPM06 Dual-Ported Memory	40042281	D	SBC6_DPM CPLD: 9093077-10
HFC-DI16I 16-Channel Digital Input Module	40045281	C	Firmware: 9120686-14
HFC-DO8J 8-Channel Relay Digital Output Module	40045701	C	Firmware: 9120677-14
HFC-DC33 Digital I/O Module w/ 2 120 VAC Digital Output Channels	40046281	E	Firmware: 9120943-10
HFC-DC34 Digital I/O Module w/ 2 125 VDC Digital Output Channels	40046781	F	Firmware: 9120944-10
HFC-AI4K 4-Channel Pulse Input Module	40044701	C	Firmware: 9120683-14
HFC-AI16F 16-Channel Analog Input Module	40043201	C	Firmware: 9120680-18
HFC-AO8F 8-Channel Analog Output Module	40047201	B	Firmware: 9120679-16
HFC-AI8M 8-Channel 100Ω RTD Input Module	40044281	D	Firmware: 9120682-14
HFC-ILR06 I/O Link Fiber-Optics Repeater/Terminator	40040201	C	

Since the scope of the TR addresses the suitability of the generic platform for general safety-related use, no specific system architecture based on the HFC-6000 platform is prescribed for any particular safety-related application. In its response to Request for Additional Information (RAI) Part 3 (References 17 and 18), HFC presented a representative system architecture illustrating how the HFC-6000 platform could be implemented in a four-channel safety system. Figure 1 (adapted from Reference 18) depicts one example of a four-channel configuration based on the HFC-6000 platform.

The expanded view of Channel A in Figure 1 further illustrates how the HFC-6000 can be used to compose one redundancy in a parallel-redundancy system architecture. It is noted that this example architecture is intended to illustrate the capability of the HFC-6000 platform to implement a prospective system architecture and does not define a proposed usage.

This red box should extend to cover the other remote and Safety C-Link

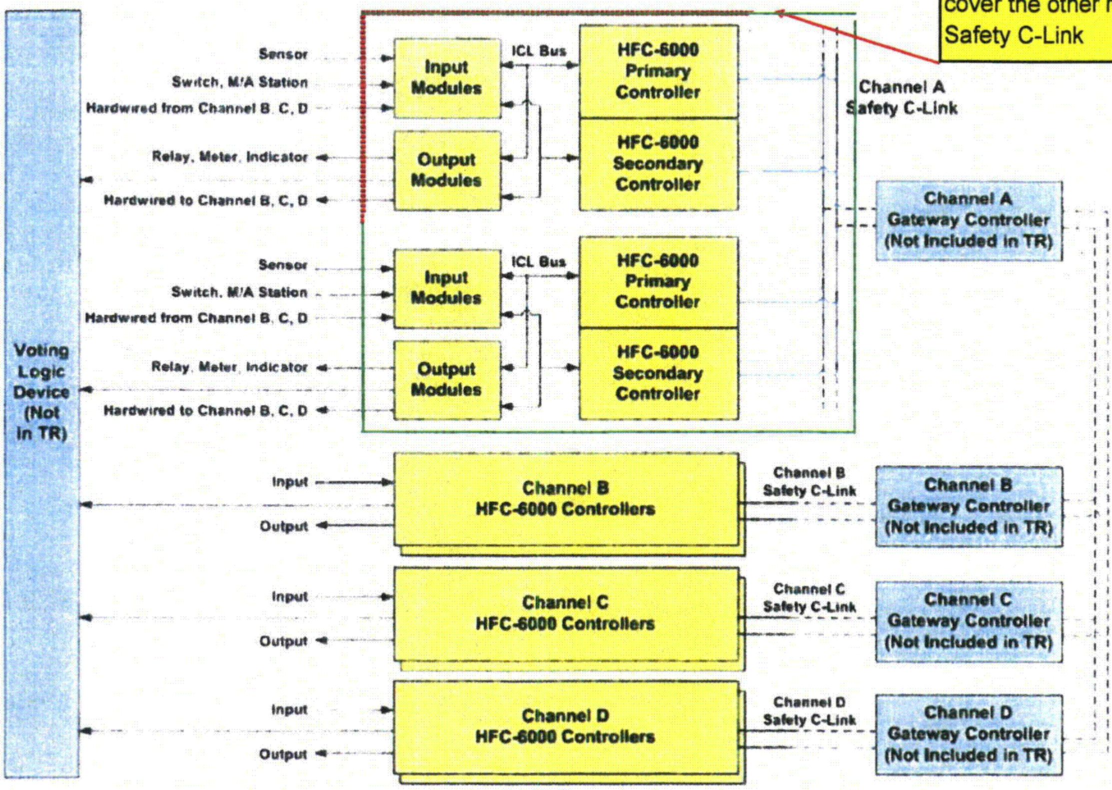

Figure 1 – Safety System Architecture Example Based on HFC-6000 Platform [Note: Only the components contained within the dashed-line box are within the scope of the topical report evaluation. Inter-channel communications has not been reviewed or approved.]

controllers, I/O

The scope of the HFC-6000 platform is indicated in Figure 1 by a dashed box around the modules, bus, and interfaces illustrated for one node of Channel A. The dedicated I/O modules serve as field device interfaces providing point-to-point interconnection to sensors, voting logic and/or actuators, and human-machine interface (HMI) displays and input devices, including manual and automatic (M/A) control interfaces. These peripheral and field devices, as well as any inter-channel connections, are outside of the as reviewed

scope of the HFC-6000 platform. Thus, other than local indication via light-emitting diodes (LEDs) and setting switches on module faceplates, displays and control interfaces are not within the scope of the HFC-6000 platform. The presence and nature of the point-to-point interconnections among safety channels that is illustrated in the figure depends on a specific system design and is outside the scope of the TR.

redundant

Regarding communication links other than the point-to-point interconnections indicated for field devices, the platform provides the redundant intercommunication link (ICL) bus and the communication link (C-Link) network. The ICL provides a redundant communication bus between the redundant controllers and I/O modules within the main and extended chassis. The ICL is fully encompassed within the scope of the platform. The C-Link, designated as the Safety C-Link in Figure 1, provides a redundant internal network to interconnect platform nodes. While the network interface for the HFC-6000 controller is an integral element of the platform, the fiber optic network medium, including the fiber optic transmitters that provide electrical-to-optical coupling, are not within the scope of the platform. Also, the gateway controller indicated as a node on the C-Link is not within the scope of the platform. Thus, the ability to connect a channel using the HFC-6000 platform with other HFC-6000 based channels or other systems, either safety-related or nonsafety-related, is not included within the scope of the platform and is not included in this evaluation.

The supporting documentation provided by HFC incorporates much of the HFC-6000 Product Line documentation as well as QA plans and qualification reports. Beginning with the top level RS901-000-01, “Product Line Requirements Specification” (Reference 19), the hierarchical relationship among the product line documents involves module requirement specifications, module design descriptions, module detailed design specifications, and component specifications (Reference 20). In addition, test procedures, review reports, and user’s guides are part of the product line documentation. The docketed materials also include qualification and CGD documents as well as QA plans. The information contained within these documents was considered as clarifying material in support of this review.

Some of the documents docketed in support of this review contain information about components, modules, and functionality that are not within the scope of the HFC-6000 platform covered by the TR. These items relate to more general features and usage of the HFC-6000 Product Line and should not be considered as an expansion of the approved platform scope. Unless clearly incorporated as an integral part of the base platform cited for safety-related application in the TR or explicitly addressed in this SE, these items were not reviewed and are not implicitly approved. As an example, peer-to-peer communication across the internal network used to interconnect instances (i.e. nodes) of the HFC-6000 platform is prohibited by design convention for a safety-related application (References 17 and 21). Although Universal Communication Protocol (UCP) functionality is extensively described in the supporting documentation (References 21 and 22), its use is restricted to offline, out-of-service maintenance activities and limited online, in-service inter-processor communication that is internal to the platform (Reference 17). Thus, UCP messages for peer-to-peer (i.e., inter-channel) communication across the C-Link network are not addressed in this review.

2.2 Regulatory Criteria

The acceptance criteria used as the basis for this review are defined in NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," Revision 5, dated March 2007. NUREG-0800, which is hereafter referred to as the Standard Review Plan (SRP), sets forth a method for reviewing compliance with applicable sections of Title 10 of the *Code of Federal Regulations* (10 CFR) Part 50, "Domestic Licensing of Production and Utilization Facilities" and 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants." Specifically, SRP Chapter 7, "Instrumentation and Controls," addresses the requirements for instrumentation and control (I&C) systems in nuclear power plants based on light-water reactor designs. The procedures for review of digital systems applied in this evaluation are principally contained within SRP Chapter 7 and are augmented and supplemented by Interim Staff Guidance.

The suitability of a digital platform for use in safety systems depends on the quality of its components; quality of the design process; and system implementation aspects such as real-time performance, independence, and online testing. Because this equipment is intended for use in safety systems and other safety-related applications, the submitted TR was evaluated in accordance with the provisions of Institute of Electrical and Electronics Engineers (IEEE) Standard (Std) 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," based on the guidance contained in SRP Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std 603," and Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std 7-4.3.2," which provide acceptance criteria for these two standards.

SRP Chapter 7, Table 7.1, "Regulatory Requirements, Acceptance Criteria, and Guidelines for Instrumentation and Control Systems Important to Safety," identifies design criteria and regulations from 10 CFR Part 50 that are applicable to I&C systems and are relevant for general review of the suitability of a digital I&C platform for generic safety-related applications. Many of the review criteria of the SRP depend on the design of an assembled system for a particular application, whereas the TR presents the elements of hardware and system software in the HFC-6000 platform that can be used in any safety application. Since no specific application of the platform as a safety system is defined, this SE is limited to review of compliance with the relevant regulations and guidance documents to the degree to which they can be satisfied at the platform level. In effect, fulfillment of system-level requirements can only be evaluated in part based on the capabilities and characteristics of the platform under review.

Determination of full compliance with the applicable regulations remains subject to plant-specific review of a full system design based on the HFC-6000 platform. Thus, it is an ASAI to establish full compliance with the applicable design criteria and regulations identified in SRP Chapter 7, Table 7.1, that are relevant to specific applications of digital I&C systems at the time the application is submitted. This and other ASAIs identified in this SE are documented in Section 3.0 and complied in Section 5.2 as plant-specific action items.

Considering the scope of the HFC-6000 platform, the following regulations and design criteria in 10 CFR Part 50 are currently determined to be applicable in whole or in part for general review of the suitability of this I&C platform for generic safety-related applications:

- 10 CFR 50.55a(a)(1), requires that "[s]tructures, 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), "Protection and safety systems," approves the 1991 version of IEEE Std 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," for incorporation by reference, including the correction sheet dated January 30, 1995
- 10 CFR Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants"
    - General Design Criterion (GDC) 1, "Quality standards and records"
    - GDC 2, "Design bases for protection against natural phenomena"
    - GDC 4, "Environmental and dynamic effects design bases"
    - GDC 13, "Instrumentation and control"
    - GDC 20, "Protection system functions"
    - GDC 21, "Protection system reliability and testability"
    - GDC 22, "Protective system independence"
    - GDC 23, "Protective system failure modes"

- 10 CFR Part 50, Appendix B, "QA Criteria for Nuclear Power Plants and Fuel Reprocessing Plants"

SRP Chapter 7, Table 7.1, identifies regulatory guides (RGs), branch technical positions (BTPs), and industry standards that contain information, recommendations, and guidance and, in general, provide an acceptable basis to implement the above requirements for both hardware and software features of safety-related digital I&C systems. Based on the scope of the HFC-6000 platform and the limitations of a platform-level review, the following guides and positions are determined to be relevant for consideration in this SE:

- RG 1.100, Revision 2, "Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants," which endorses IEEE Std 344-1987, "IEEE Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generation Stations"
- RG 1.152, Revision 2, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," which endorses IEEE Std 7-4.3.2-2003, "Standard Criteria for Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations"
- RG 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std 1012-1986, "IEEE Standard for Software Verification and Validation Plans," and IEEE Std 1028-1988, "IEEE Standard for Software Review and Audits"

- RG 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std 828-1990, "Software Configuration Management Plans," and IEEE Std 1042-1987, "IEEE Guide to Software Configuration Management"
- RG 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std 829-1983, "IEEE Standard for Software Test Documentation"
- RG 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses ANSI/IEEE Std 1008-1987, "IEEE Standard for Software Unit Testing"
- RG 1.172, "Software Requirements Specification for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std 830-1993, "IEEE Recommended Practice for Software Requirements Specifications"
- RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes"
- RG 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," which endorses IEEE Std 1050-1996, "IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations," and specified test methods from MIL-STD-461E, "Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment" and International Electrotechnical Commission (IEC) 61000 series of electromagnetic interference and radio-frequency interference (EMI/RFI) test methods
- RG 1.209, "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants," which endorses IEEE Std 323-2003, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations"
- SRP BTP 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems"
- SRP BTP 7-17, "Guidance on Self-Test and Surveillance Test Provisions"
- SRP BTP 7-21, "Guidance on Digital Computer Real-Time Performance"
- DI&C-ISG-04, "Interim Staff Guidance on Highly-Integrated Control Rooms – Communications Issues (HICRc)," September 28, 2007.

Since the HFC-6000 is an existing commercial off-the-shelf (COTS) digital I&C platform, certain industry guidelines that address dedication and qualification processes are applicable. The NRC staff has reviewed and accepted the following industry guidance documents based on conditions established in safety evaluation (SE) reports.

- Electric Power Research Institute (EPRI) Topical Report (TR)-102323, "Guidelines for Electromagnetic Interference Testing in Power Plants," as accepted by the NRC SE dated April 30, 1996

- EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," as accepted by the NRC SE dated April 1997
- EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," as accepted by the NRC SE dated July 30, 1998

It should be noted that industry standards, documents, and reports use the word "requirements" to denote provisions that must be implemented to ensure compliance with the corresponding document. Additionally, these standards, documents, and reports provide guidance or recommendations that need not be adopted by the user to ensure compliance with the corresponding document, and the optional items are not designated as "requirements." The word "requirement" is used throughout the I&C discipline. However, licensee or vendor documentation of conformance to the "requirements" provided in industry standards, documents, and reports referenced in this SE only constitutes conformance with NRC regulatory requirements insofar as endorsed by the NRC. Furthermore, use of the word "requirements" in these documents does not indicate that the "requirements" are NRC regulatory requirements.

2.3 Precedents

Three TRs for digital platforms have previously been submitted to the NRC for review and approval. These platforms are the AREVA TELEPERM XS (TXS), the Westinghouse Common Q, and the Invensys Tricon, and they were generically qualified in accordance with the approved guidance of EPRI TR-107330. The corresponding SEs (References 23, 24, and 25) for these platforms document the findings of the reviews by NRC staff and constitute applicable precedents that are considered in the conduct of this review. Additionally, a recent SE documents a license amendment review for the implementation of a field-programmable gate array (FPGA) platform for a safety application at the Wolf Creek Generating Station (Wolf Creek) (Reference 26). The Wolf Creek application includes extensive platform-specific material, so it also serves to provide relevant regulatory precedent applicable for the review of platform TRs. The SE regarding the Oconee Nuclear Station reactor protective system and engineered safeguards protective system (RPS/ESPS) (Reference 27) provides the most recent example of an evaluation of a digital safety system against NRC's safety regulations and guidance.

Specific precedents employed to support this review address environmental qualification, exceptions to key performance requirements specified by EPRI TR-107330, and CGD of PDS. Each of the SEs for the generic platforms (i.e., TXS, Common Q, and Tricon) addresses deficiencies in the environmental qualification program for the respective platforms either through treatment as generic open items or identification of a commitment to retest on a plant-specific basis. The SE for the Tricon platform (Reference 25) provides a precedent for the treatment of exceptions to the response time performance requirement from EPRI TR-107330. The SE for the Common Q platform (Reference 24) provides an evaluation of dedication activities by Combustion Engineering Nuclear Power (now owned by Westinghouse) for commercial grade items, including software, that are used in the platform. The commercial dedication of a Siemens-designed, application-specific integrated circuit (ASIC) for use as the system support controller on platform PCBs provides a precedent from the SE for the TXS platform (Reference 23) regarding the treatment of custom chips that provide processor support functionality for board management.

3.0 TECHNICAL EVALUATION

This SE follows the guidance contained in SRP Chapter 7. Chapter 7 of the NRC SRP provides guidance on reviewing complete nuclear power plant designs of I&C systems. Revision 5 to SRP Chapter 7 also includes review criteria for digital systems. The guidance is applicable to the review of TRs for evaluating the suitability of generic digital platforms for safety-related use through consideration of general system requirements. Based on examination of SRP Chapter 7, Table 7-1, Appendix 7.0-A, "Review Process for Digital Instrumentation and Control Systems," and Appendix 7.1-A, "Acceptance Criteria and Guidelines for Instrumentation and Control Systems Important to Safety," the relevant regulatory requirements, BTPs, Interim Staff Guidance (ISG), and acceptance criteria that can be addressed in part at the platform level are identified in Section 2.2 of this SE. The evaluation of the HFC-6000 platform against the identified acceptance criteria is documented in the following subsections.

The evaluation described in this section is based on review of the information contained within the TR. The HFC-6000 platform is described in Sections 5, 6, and 7 of the TR. Section 8 of the TR contains discussion of key safety system design topics, such as quality assurance, independence, deterministic performance, security, and reliability, as well as an assessment of compliance with regulations, codes, standards, and guidance for digital I&C systems. In the TR, environmental qualification is covered in Section 9 and software qualification is addressed in Section 10. The material contained in these sections of the TR was the principal focus of the SE and is the primary source of the descriptive information on the HFC-6000 platform presented in this section. Supplemental documentation docketed by HFC provides supporting and/or clarifying information that was considered in this evaluation. Specific reference to the source document is given where key information or supporting evidence from any of these additional documents proved to be essential to the conduct of the evaluation.

3.1 HFC-6000 Platform Description

The HFC-6000 platform is composed of PLC modules with associated I/O and communication components. To support safety-related applications, a single channel can be implemented based on one or more HFC-6000 platforms interconnected via an internal (i.e., intra-channel) redundant communication network employing a token-passing protocol. Application-specific system architectures, communication interconnections among safety system redundancies (e.g., channels or divisions) and/or with external systems, displays, indicators, input devices and other HMIs, and application software are not included in the scope of the HFC-6000 platform TR submitted for review.

The base HFC-6000 platform consists of equipment chassis, power supplies, controller modules, I/O modules, and communication interfaces, as well as the associated operating software.

Table 1 in Section 2.1 of this SE identifies the specific components that constitute the HFC-6000 platform under review. Typical platform configurations include redundant controllers and a specific set of I/O modules housed in a main equipment chassis. Expansion equipment chassis enable configuration of additional I/O modules.

The HFC-6000 controller and I/O modules are microprocessor based PCBs with operating software installed in firmware. The HFC-6000 controller provides process execution of predefined logic programs, performs periodic I/O scans, and broadcasts status information. The I/O modules provide the hardware interface to field devices such as sensors, relay logic, and actuators. Collectively, the I/O modules can handle multiple strings of both digital and analog signals based upon the use of specific types of I/O devices.

The HFC-6000 platform provides dedicated processors within the controller module to manage communication interfaces. These communication interfaces support transmission of data between the controller and I/O modules and transfer of information among separate safety controllers within a safety channel (i.e., a single redundancy of a safety system). Communication between controller and I/O modules is accomplished serially across redundant backplane interconnections designated as the intercommunication link or ICL. Communication among safety platforms is accomplished via redundant network connections designated as the communication link or C-Link. The C-Link communication provides a means for a controller to broadcast data and exchange status information with other controllers in the same channel.

The HFC-6000 platform software consists of controller software, I/O software, communication software, and test and diagnostic software that constitute a dedicated subset of the operating software library that has been previously implemented by HFC for numerous industrial and nuclear power plant applications.

3.1.1 Hardware Description

The hardware components for the HFC-6000 platform are as follows:

- Controller backplane for 19-inch equipment chassis, HFC-BPC01-19;
- Expansion backplane for 19-inch equipment chassis, HFC-BPE01-19;
- 24 volt (V) power supply module, HML 601-5;
- 48 V power supply module, HML 601-8;
- Controller module, HFC-SBC06;
- Dual-ported memory module, HFC-DPM06;
- Digital input module, HFC-DI16I;
- Relay output module, HFC-DO8J;
- Digital control module for motor operated valves, HFC-DC33;
- Digital control module for electrically operated breakers, HFC-DC34;
- Pulse input module, HFC-AI4K;
- Analog input module, HFC-AI16F;
- Analog output module, HFC-AO8M;
- Resistance temperature detector input module, HFC-AI8M; and
- I/O link fiber-optics repeater/terminator, HFC-ILR06.

Figure 2, which was extracted from Figure 2 of Reference 28, illustrates a typical arrangement of modules for the HFC-6000 platform. As shown, the controller and I/O modules (IOMs) are housed in the main equipment chassis with additional IOMs implemented in an expansion equipment chassis. The configuration of the HFC-6000 platform also includes power supply modules (PSMs) in a separate power rack that provides redundant 24 volts of direct current (VDC) and 48 VDC power via separate backplane traces in each equipment chassis.

The figure illustrates a redundant configuration of system controllers, which includes two HFC-SBC06 controller modules and one HFC-DPM06 dual-ported memory module. The redundant controller assembly constitutes the base central processing unit (CPU) module (CPUM) for the safety platform. In the CPUM configuration, one module acts as the primary (i.e., active) controller and the other module serves as secondary (i.e., hot standby) controller.

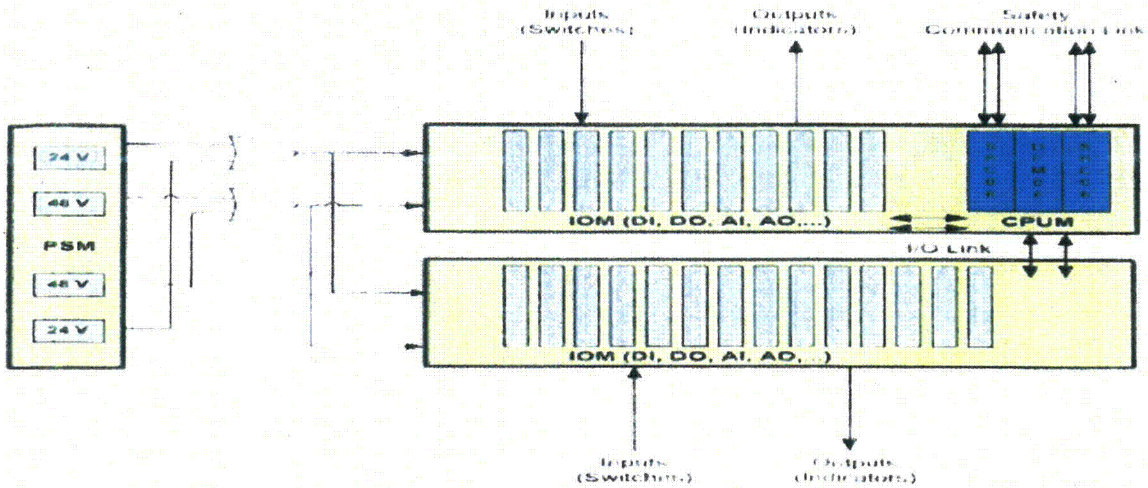

Figure 2 – Hardware arrangement for HFC-6000 platform

The I/O capability of the HFC-6000 platform is provided by a collection of different modules to provide the appropriate I/O interfaces based on signal type. Each IOM has a serial I/O communication path to the controllers via the redundant ICL bus. Within the redundant controller configuration, each ICL logical link is allocated to a separate controller module to allow each IOM to connect with both controllers via the separate ICL paths. The connection to the ICL Bus for IOM in the expansion chassis are provided locally via twisted pair wires or remotely via fiber optic cables.

The safety communication link indicated in the figure is the C-Link network, which interconnects CPUM (i.e., safety controller nodes) to enable broadcast of data and status information among safety controllers within the same channel.

3.1.1.1 HFC-6000 Equipment Chassis

The equipment chassis for the HFC-6000 platform are rack-mounted 19-inch assemblies that house the CPUM and IOMs. The HFC-6000 equipment chassis provides connectors and electrical traces to support the HFC-6000 modules. Two basic types of chassis are provided for the HFC-6000: the controller chassis and the expansion chassis.

3.1.1.1.1 Controller Chassis Backplane – HFC-BPC01-19

HFC-BPC01-19 is the controller chassis backplane for a standard 19-inch equipment assembly. It provides two slots for HFC-SBC06 controllers, one slot for an HFC-DPM06 module, and capacity for a maximum of eleven HFC-6000 IOMs. The backplane receives operating power from the PSM via redundant power cables that attach to a connector on the back of the chassis. The 24 VDC operating power and 48 VDC auxiliary power are routed to each module via dual power rails on the backplane. Each HFC-6000 module performs diode auctioneering of the redundant power as well as voltage level conversion to obtain the operating power needed for onboard hardware. The CPUM communicates with IOMs via redundant serial ICL traces on the backplane. Redundant ICL connectors on the rear of the backplane enable extension of the ICL bus to local expansion chassis by twisted pair ICL cable or to remote expansion chassis through an optical repeater.

3.1.1.1.2 Extension Chassis Backplane – HFC-BPE01-19

HFC-BPE01-19 is an I/O expansion chassis backplane for a standard 19-inch equipment assembly. It provides slots for a maximum of 14 HFC-6000 IOMs. As is the case for the controller chassis backplane, the expansion chassis backplane receives operating power from the PSM via redundant power cables that attach to a connector on the back of the chassis. Dual power rails on the backplane route the redundant power to each IOM for diode auctioneering and voltage level conversion. The ICL cables connected to a controller chassis mate with corresponding connectors on the back of the expansion chassis backplane, and ICL traces are routed from the connectors to each card slot. For local installation, twisted pair cable provides local interconnection, while fiber optic cabling employing optical repeaters/terminators is used for remote interconnection.

3.1.1.2 HFC-6000 Power Supply Module – 600W 24V Power Supply and 600W 48V Power Supply

Power for the HFC-6000 platform is provided by a rack-mounted PSM with slots for separate power supplies. The PSM provides a split rack configuration that can accommodate up to eight separate (i.e., four redundant) power supply assemblies. Groupings of up to four power supply assemblies constitute redundant internal power divisions that can each be separately driven by an independent alternating current (AC) power source. The two power groups provide 24 VDC and 48 VDC to supply parallel power rails in the HFC-6000 equipment chassis. The 24 VDC power rails are diode auctioneered within each HFC-6000 module to produce onboard logic power. The 48 VDC power rails supply excitation voltage for external relay contacts and field transducers. Each power group accepts input from a single phase AC power source ranging from 90-264 V, 47-63 hertz (Hz) and provides a typical output rating of 50 amperes (A) at 24 VDC and 12.5 A at 48 VDC (Reference 29). The power capacity of this arrangement is more than adequate to supply redundant operating power for a typical implementation of HFC-6000 equipment chassis in a single cabinet.

The power supply assemblies are commercial grade items supplied by Jasper Electronics (Reference 17). The HML601-5 (24 V) and HML601-8 (48 V) power supplies, HFC part numbers 9044524Q and 9044525Q respectively, have been commercially dedicated by HFC (Reference 18). The power supply assemblies are hot swappable, and provide under-voltage, over-voltage, over-current/short, and over-temperature protection. Remote sense compensation for line loss and hold up time capabilities are also provided. Also, power fail and under-voltage warning signals are available.

3.1.1.3 I/O Link Fiber-Optics Repeater/Terminator – HFC-ILR06

As described in Section 3.1.1.1 of this SE, the ICL bus interconnection between a controller chassis and a remote expansion chassis is provided by fiber optic cabling employing optical repeaters/terminators. Within a chassis, the IOMs have onboard transceivers for communication across the backplane. Redundant backplane connectors allow extension of the ICL bus from a controller chassis to an expansion chassis. HFC-ILR06 I/O Link Fiber-Optics Repeater/Terminator modules provide the electrical-to-optical coupling to enable fiber optic communication with IOMs installed in a remote expansion chassis.

3.1.1.4 Controller Module – HFC-SBC06

As illustrated in Figure 2, the redundant configuration of controllers that constitute the CPUM of the safety platform involves two HFC-SBC06 controller modules and one HFC-DPM06 dual-ported memory module. The HFC-SBC06 controller module is the principal component of the CPUM within the HFC-6000 platform, with one module serving as the active or primary controller and the other module serving as the secondary or backup controller. Specifically, the HFC-SBC06 controller module, when acting as the primary controller for the safety CPUM, is the safety system controller on which safety functions are implemented. In its role as primary controller, the HFC-SBC06 provides execution of predefined application programs, performs periodic I/O scans, and enables broadcast communication among network nodes (i.e., other HFC-6000 CPUM within a channel). In addition to its operational functions, the HFC-SBC06 also provides failure detection and failover indication.

The HFC-SBC06 controller module has a 64-bit system (SYS) processor and two 32-bit subordinate processors to provide the execution environment for safety applications and perform all computational, diagnostic, and communication functions. The SYS processor is an Intel Pentium microprocessor while the subordinate processors are Intel 386EX microprocessors. The two subordinate processors are the ICL processor and the C-Link processor. [

]

Power is supplied to the controller module via the dual power rails of the controller chassis backplane, HFC-BPC01-19. The redundant 24 VDC power is diode auctioneered and routed to two power regulators that provide 5 VDC and 3.3 VDC power for module operation.

[

]

The HFC-SBC06 module contains eight board-edge LEDs, which provide a visual indication of the status of the controller hardware and software. It also provides one eight-position dual in-line package (DIP) switch, two toggle switches and nine jumpers. The switches and jumpers enable manual control of reset, hardware configuration, and programming of the board. In particular, the switches provide for power on/off control and write protect control for the application code stored in onboard Flash memory.

The operating modes of the HFC-SBC06 module are switch selectable. The four settings are:

- RUN → Normal operating mode
- SIMULATION → Offline application simulation mode
- OFFLINE → Offline application loading mode
- TEST → Offline diagnostic test mode

The RUN or normal operating mode of a controller consists of sequential execution of the application program and predefined utilities under control of the operating system (OS). The other three operating modes (SIMULATION, OFFLINE, and TEST) are not intended for online, in-service use in plant systems. [

]

3.1.1.5 Dual-Ported Memory Module – HFC-DPM06

The dual-ported memory (DPM) array on the HFC-DPM06 module is accessible to both the primary and secondary controllers. The module interconnects the two redundant controllers to provide the mechanisms that enable primary and secondary control status to be established for the redundant HFC-SBC06 controller modules and also facilitate failover of primary control status from one controller to the other based on manual demand or failure detection. [

]

3.1.1.6 Input/Output Modules

The HFC-6000 IOMs provide the signal-level interface to the field devices that are being monitored or controlled. The major functions performed by the HFC-6000 IOMs are to receive input signals and set output signals, communicate with redundant HFC-SBC06 controllers via the ICL bus, and perform self-diagnostic monitoring. The multi-channel IOMs handle both digital and analog signals based upon the types of I/O devices. The IOMs include a digital input module, a relay output module, two special purpose, multi-channel I/O modules designed for nuclear power plant applications, a pulse input module, an analog input (AI) module, an analog output (AO) module, and a resistance temperature detector (RTD) input module.

[

]

3.1.1.6.1 Digital Input Module – HFC-DI16I

The HFC-DI16I module provides a digital input (DI) for up to sixteen digital or discrete field devices. The module reads the digital data from its input channels during each data scan interval and stores the data in onboard memory for subsequent communication to the primary controller in response to polling.

[

]

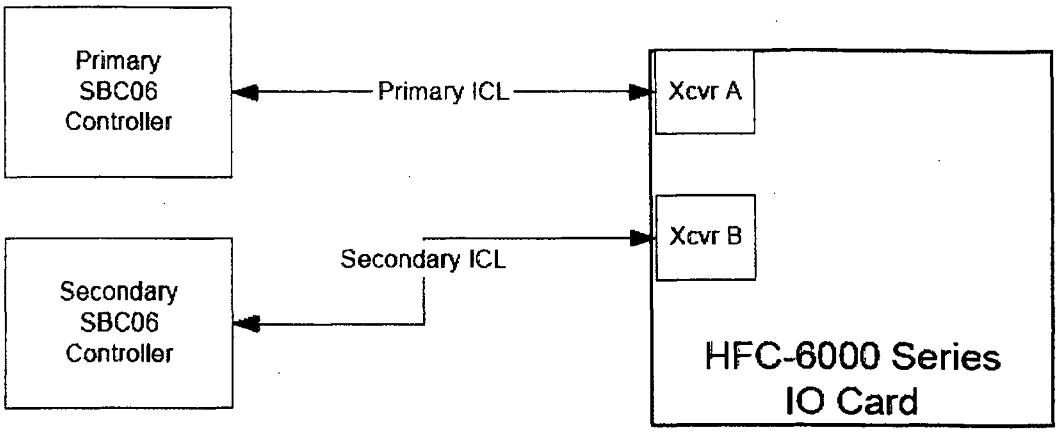

Figure 3 – IOM serial bus connections with redundant HFC-SBC06 controllers

3.1.1.6.2 Relay Output Module – HFC-DO8J

The HFC-DO8J module provides a relay digital output (DO) for up to eight field devices. The module receives the digital output data from the primary controller during each polling intervals (i.e., the frequency at which data is requested/transmitted) and uses this data to set the on/off status of each output relay. The ON/OFF output data for the eight channels are held in memory as a single byte of data.

[

]

3.1.1.6.3 Digital I/O Controller Module for Motor Operated Valves – HFC-DC33

The HFC-DC33 provides a special purpose, multi-channel I/O buffer and controller capability for the HFC-6000 platform that is designed for nuclear power plant applications. The module is used for control, interrogation, and monitoring of field devices. The buffer is specifically designed to satisfy the control requirements of a dual-coil MOV starter. The module provides twelve general-purpose DI channels, two 120 VAC DO channels, and onboard status sensing for monitoring coil continuity, overloads, and valve position.

eleven

[

]

3.1.1.6.4 Digital I/O Controller Module for Electronically Operated Breakers – HFC-DC34

The HFC-DC34 module provides a multi-channel I/O buffer and controller capability for the HFC-6000 platform. It is used for control, interrogation, and monitoring of field devices. Typical applications include monitoring electrically-operated breakers (EOB) for overloads. This module is designed to provide the specific combination of digital I/O channels needed to control motor starters or switchgear field equipment. The module provides eleven general-purpose DI channels, two 125 VDC DO channels, and onboard status sensing for monitoring coil continuity and overloads.

[

]

3.1.1.6.5 Pulse Input Module – HFC-AI4K

The HFC-AI4K module provides four input channels for processing pulse signals from field equipment. The four channels are organized as two pairs. Configuration parameters for each channel pair can be entered using switches that are accessible at the front bezel of the module. These configuration parameters permit selection of rate or accumulate mode. Specifically, onboard slide switches provide the means for selecting between rate and accumulate mode for each channel pair. When the rate mode is selected for a particular pair of channels, hardware counters produce a count value that represents the frequency of the input signal. When the accumulate mode is selected, the counter increments with each input pulse, and the onboard processor scales the input based on a pre-scaled value. [

]

[

]

3.1.1.6.6 Analog Input Module – HFC-AI16F

The HFC-AI16F module provides an AI interface for up to sixteen analog field inputs. The module receives the 4-20 mA analog signals, performs analog-to-digital conversion for each channel during each data scan interval, and stores the resulting digital data in onboard memory for subsequent communication to the primary controller in response to polling.

[

]

3.1.1.6.7 Analog Output Module – HFC-AO8F

The HFC-AO8F module provides an AO interface for up to eight analog field devices. The module receives digital data from the primary controller during each polling interval and performs digital-to-analog conversion for each 4-20 mA output channel. The HFC-SBC06 controller initiates communication with a configured HFC-AO8F module during its regular polling while the HFC-AO8F module receives the current digital data for all output channels from the poll message and returns current status.

[

]

The HFC-AO8F module provides the capability to set a failsafe condition for each channel to account for failures in ICL communication or watchdog timeout. Jumper settings are used to configure the board for one of thee failsafe modes: fail high, fail low, or hold last state.

3.1.1.6.8 RTD Input Module – HFC-AI8M

The HFC-AI8M module is an input-conditioning device for the HFC-6000 platform. The module supports measurement based on 100Ω platinum RTDs with each channel designed to accept either a two- or a three-wire RTD sensor. The HFC-AI8M module receives the voltage signals of its isolated AIs from up to eight external RTD wires and samples the signals for conversion into digital count value data for each channel during each scan interval. The digital data is subsequently communicated to the primary controller in response to polling.

[

]

3.1.2 Communication Interfaces

The HFC-6000 platform provides communication interfaces to support transmission of data between the CPUM and IOMs and transfer of information among safety controllers within a channel. The purpose of the first type of communications is to allow periodic polling to update I/O data. The purpose of the second type of communications is to provide status information and operational data from one safety node (i.e., a single instance of the HFC-6000 controller or CPUM) in a channel to other safety nodes in the same channel (e.g., interconnected CPUM within a single redundancy for a safety system). Figure 4 (which was extracted from Figure 3 of Reference 30) shows the communication interfaces within the HFC-6000 platform.

[

]

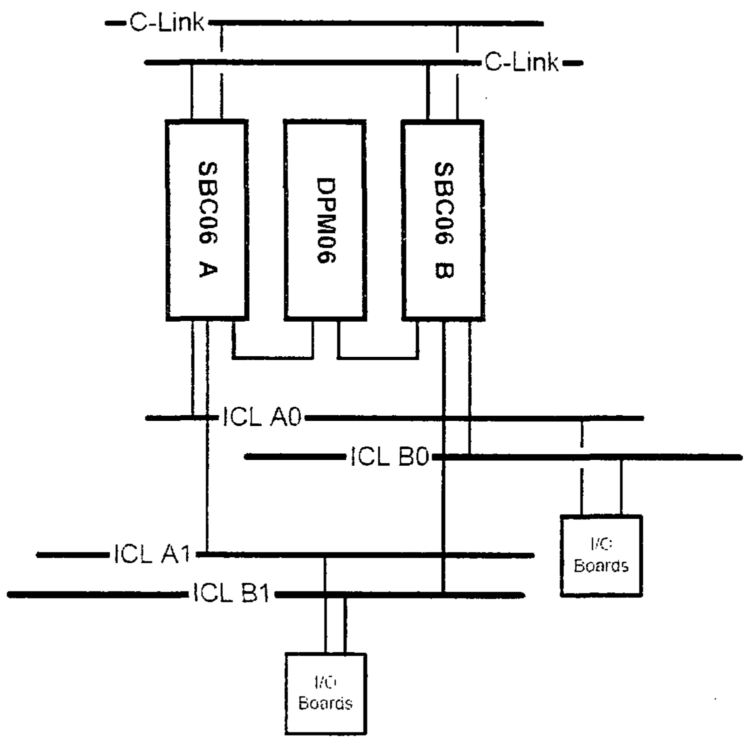

Figure 4 – HFC-6000 platform communication interfaces

3.1.3 Software Description

The software that will be utilized for safety-related application of the HFC-6000 platform is broken down into two categories: (1) Operating Software and (2) Application Software (Plant Specific).

Operating software consists of the system services, basic functions, and execution environment that form the general computational capability of the HFC-6000 platform. The operating software is installed in firmware associated with each processor on the various platform modules. This operating software is coded in assembly language and stored in non-volatile memory (PROM and Flash memory). The firmware is installed at the factory and cannot be altered by the end user. The HFC-6000 operating software comprises the base software of the platform and is commercially dedicated as PDS.

Application software consists of plant-specific programs that provide the unique functionality required for a safety-related application. Application software is stored in non-volatile memory (PROM or Flash memory) and is transferred to RAM during controller power-up initialization for subsequent execution during online operation. Switch-enabled write protection prevents alteration of the application software while the controller is operating in the online mode. Application software is created or modified using software development tools on an Engineering Workstation (EWS) and can be installed while the controller is offline and out of service (i.e., not installed in the field cabinetry). Since a specific safety application is not established for the HFC-6000 platform, the application software, software development tools, and software development plans are not within the scope of this review.

The scope of the HFC-6000 platform, as discussed in Section 2.1 and indicated in Table 1 of this SE, identifies the operating software in terms of the firmware associated with each processor type for the base modules. Specifically, the three processors of the HFC-SBC06 controller module are the SYS, ICL, and C-Link processors. The operating software corresponding to each processor is identified as the System Controller Program (SC) firmware, Subordinate Asynchronous Program (SAP) firmware, and Subordinate Ethernet Program (SEP) firmware, respectively. The operating software for each IOM is identified with the corresponding IOM firmware.

In addition to the operating software, the onboard CPLDs for the HFC-SBC06 and HFC-DPM06 modules are explicitly identified in the list of components for the HFC-6000 platform (see Table 1 in this SE). The five identified CPLDs are custom chips that HFC designed to provide "hardwired" board management mechanisms and support for the redundancy and failover capabilities of the platform. The logic source code is implemented using the very-high-speed integrated circuit (VHSIC) hardware description language (VHDL). As confirmed in the HFC response to RAI Part 3 (Reference 17), the VHDL logic code for the CPLDs is treated in accordance with the defined life cycle processes of the HFC software QA program. Thus, the software description of HFC-6000 platform within this section also includes a discussion of the board management functionality instantiated in the VHDL logic code for each CPLD.

In addition to the information presented in the TR, the description of the operating software that follows incorporates clarifying information from the following supplemental HFC documents.

[

]

3.1.3.1 Board Management Logic (CPLD Chips)

[

]

3.1.3.2 Operating Software

The operating software for the HFC-6000 platform consists of a generic real-time operating system (OS), utility service tasks, and basic modules and functions that serve as the basic elements of application software. [

]

3.1.3.2.1 Operating System Software

The HFC OS is a fundamental HFC software component. [

]

3.1.3.2.2 SYS Processor Software (SC Firmware)

The SYS processor monitors overall status of the controller module, services software watchdog timers, services the hardware watchdog timer, and executes the application program code. Monitoring the status of the controller module includes coordination of the two subordinate processors and interaction with the redundant controller through the DPM.

[

]

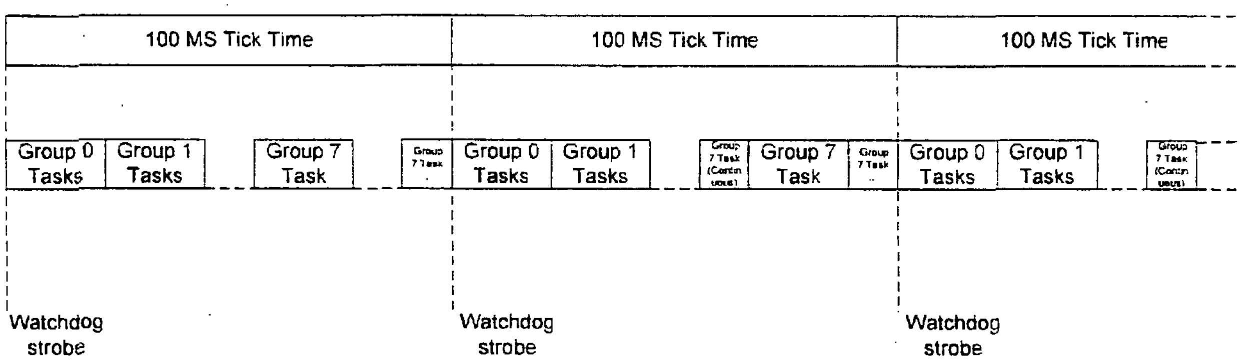

Figure 5 – Execution of software tasks

3.1.3.2.3 ICL Processor Software (SAP Firmware)

[

]

3.1.3.2.4 C-LINK Processor Software (SEP Firmware)

The C-Link processor controls overall operation of the communications interface to the C-Link. It manages the transmission of data to or from the network as well as the transfer of data to and from the public memory of the controller module. [

]

3.1.3.2.5 I/O Module Software (IOM Firmware)

The HFC-6000 IOMs serve as the interface between the platform and field devices. Their primary function is either the acquisition of input signals or the transmission of output signals. The IOMs also communicate with the controller module.

[

]

3.1.3.3 Application Software Architecture

An application is implemented as a SYS processor software task based on the EI. The program itself consists of an assemblage of individual logic subroutines and analog processing algorithms coupled with application configuration data. [

]

3.1.3.4 Software Development Tools

The development tools for the PDS of the HFC-6000 platform are described in Section 7.3 of the TR. The operating software for the controller modules and IOMs of HFC-6000 platform software is written in Intel Assembly language. The code was originally developed using the Intel x86 Cross Assembler, Linker and Locater on a Digital Equipment Corporation (DEC) VAX computer. In recent years, HFC migrated the operating software development process from the VAX-based software development environment to a PC-based software development environment. Code management is implemented using Microsoft SourceSafe, with the Serena PVCS Version Manager software tool providing configuration management. Code development is performed using Microsoft Visual Studio. All the code needed to build the software for an HFC-6000 controller is in SourceSafe project folders. [

]

3.2 Software Documentation

The regulation at 10 CFR 50.55a(a)(1) requires, in part, that systems and components be designed, tested, and inspected to quality standards commensurate with the safety function to be performed. 10 CFR Part 50, Appendix B, Criterion III, "Design Control," requires in part that quality standards be specified and that design control measures shall provide for verifying or checking the adequacy of design. SRP Chapter 7, Appendix 7.0-A, Section 3.H, "Review Process for Digital Instrumentation and Control Systems," states that "All software, including operating systems, that is resident on safety system computers at runtime must be qualified for the intended applications. Qualification may be established either by producing the PDS items under a 10 CFR [Part] 50, Appendix B QA program or by dedicating the item for use in the safety system as defined in 10 CFR [Part] 21."

The HFC-6000 platform supports operating software and application software. The operating software provides the basic services and computational capabilities of the platform and is identified as being within the scope of the review. The operating software of the HFC-6000 platform is PDS that has been dedicated for nuclear-safety applications. Thus, the evaluation of the software documentation for the HFC-6000 platform primarily focused on the documentation of CGD activities and resulting evidence. The review of CGD documentation is addressed in Section 3.2.1 below.

SRP BTP 7-14, Revision 5, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems," presents review guidance and acceptance criteria in terms of planning documents, implementation process documents, and design outputs. Review of planning documents addresses the software development planning activities and products to ascertain the establishment of an acceptable high quality process. Review of implementation process documents focuses on specific life cycle process implementation activities and documentation to determine that the quality plans have been properly executed. Review of design outputs concentrates on the products of the development process that describe the end product (e.g., code, model, system) to provide confidence that the resultant software is of high quality.

Application software represents the instantiation of a safety or control function to implement a plant-specific safety-related system. While application software utilizes the functionality and services of the platform, it is not identified as being within the scope of the review but, rather, remains subject to plant-specific review for regulatory compliance. To this end, HFC has confirmed that it is not seeking approval of the application software development process or associated plans and procedures through review of the TR (Reference 14). Nevertheless, Section 10 of the TR clearly indicates that HFC will maintain the operating software of the HFC-6000 platform under its QA program, which was developed to be compliant with 10 CFR Part 50, Appendix B. Thus, the review of the HFC software QA program is limited to evaluation of software documentation as it relates to maintaining the commercially dedicated PDS.

Since the operating software of the HFC-6000 platform was developed before the establishment of the HFC software QA program and the treatment of new software development is not within the scope of the review, the structure of the evaluation differs from the organization identified in SRP BTP 7-14. The evaluation of software life cycle planning documentation focuses on aspects on the life cycle plans that are relevant to the maintenance of the PDS to preserve its suitability for nuclear safety use as established through the dedication process. This evaluation is documented in Section 3.2.2 below. With little relevant process implementation documentation available, evaluation of existing implementation documents is embedded in Section 3.2.2 with the treatment of life cycle planning documentation. Finally, Section 3.2.3 documents the evaluation of the available design outputs that correspond to the PDS, which primarily consist of the reconstituted requirements and design documents from the dedication effort.

3.2.1 Commercial Grade Dedication of Predeveloped Software Documentation

10 CFR Part 21, "Reporting of Defects and Noncompliance," states reasonable assurance that a commercial grade item will perform its intended safety function "is achieved by identifying the critical characteristics of the item and verifying their acceptability by inspections, tests, or analyses performed by the purchaser or third-party dedicating entity after delivery, supplemented as necessary by one or more of the following: commercial grade surveys; product inspections or witness at hold points at the manufacturer's facility; and analysis of historical records for acceptable performance." SRP Chapter 7, Appendix 7.0-A, Section 3.H, "Review Process For Digital

Instrumentation and Control Systems," identifies review topics concerning the dedication of a commercial item as defined in 10 CFR Part 21.

The criteria for demonstrating reasonable assurance that a computer and/or legacy software will perform its intended safety functions is established in Sub-Clause 5.4.2, "Qualification of Existing Commercial Computers," of IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations." EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," provides detailed guidance for the evaluation of existing commercial computers and software to meet the provisions of IEEE Std 7-4.3.2-2003, which was approved in RG 1.152, Revision 2. In particular, the EPRI TR provides more detail on the characteristics of an acceptable process for qualifying existing software, and discusses the use of engineering judgment and compensating factors. It is noted that the guidance of SRP BTP 7-14 may be applied to the evaluation of vendor processes described in EPRI TR-106439. In addition, EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," provides more specific guidance for the evaluation of existing PLC platforms by describing generic functional and qualification requirements and identifying compensating quality activities.

The CGD guidance provided in EPRI TR-106439 involves identifying the critical characteristics of the commercial grade digital equipment based on the safety-related technical and quality requirements, selecting appropriate methods to verify the critical characteristics to enable dedication of the digital equipment, and maintaining the dedication basis over the service life of the equipment. The guidance adapts the methods established in EPRI NP-5652, "Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications," to digital equipment and is consistent with the guidance contained in Generic Letter (GL) 89-02, "Actions to Improve the Detection of Counterfeit and Fraudulently Marketed Products," and GL 91-05, "Licensee Commercial-Grade Procurement and Dedication Programs."

Section 10.1 of the TR describes the dedication of the PDS of the HFC-6000 platform. [

]

Table 1 of Section 2.1 of this SE lists the firmware part numbers that identify the specific versions of the operating software corresponding to the platform under review.

In Section 10.1.1 of the TR, HFC claims that the successful CGD of the PDS of the HFC-6000 platform is consistent with the guidance provided in IEEE Std 7-4.3.2-2003 and EPRI TR-106439. The CGD process employed by HFC is based on the equivalent level of assurance approach defined in EPRI TR-106439. The overall PDS dedication program involved verification of software documentation, software validation and testing, and review of operating history.

EPRI TR-106439 identifies three categories of critical characteristics in terms of physical, performance, and dependability attributes. These characteristics correspond to the categories identified in Sub-Clause 5.4.2.2 of IEEE Std 7-4.3.2-2003, which are physical, performance, and development process characteristics. Determination of specific critical characteristics is accomplished by a critical design review that accounts for the requirements of the safety application and the potential hazards that could interfere with the safety function.

Generic, high-level technical (i.e., functional and performance) and quality requirements for safety-related applications are specified by EPRI TR-107330. Based on these generic requirements and its platform design, HFC performed a critical design review for the operating software components of the HFC-6000 platform to identify the critical characteristics that required verification to successfully dedicate the PDS.

Verification of the critical characteristics is at the heart of the dedication process. EPRI TR-106439 adapts four acceptance methods defined in EPRI NP-5652 to establish an approach to verify the characteristics for digital equipment. The four methods are:

- Method 1 --- Special Tests and Inspections
- Method 2 --- Commercial Grade Survey of Supplier
- Method 3 --- Source Verification
- Method 4 --- Acceptable Supplier/Item Performance Record

EPRI TR-106439 states that verification of the critical characteristics for digital equipment will require the use of more than one of the methods since no one method will typically be sufficient by itself. It is noted in the guidance that Methods 1, 2, and 4 are needed for many digital devices. As described in Section 10.1.1, the TR identifies three elements as the HFC-6000 dedication process (i.e., software verification and testing program, verification of software documentation, and operating history). Of the four acceptance methods described in EPRI TR-106439 for digital equipment, the process employed by HFC corresponds to forms of Method 1 (special tests and inspections), Method 2 (commercial grade survey), and Method 4 (acceptable performance record). Since the dedicator (HFC) is also the current vendor, the application of Method 2 involved identification of the development processes applied by the predecessor organization (Forney Corporation) in the development and history of the heritage products, with this survey augmented by development of supplemental information in the form of reconstituted software documentation. The NRC staff finds the HFC approach to CGD of PDS to be an acceptable implementation of the methodology identified in EPRI TR-106439.

To facilitate the critical design review and execution of the dedication process, HFC developed a quality process procedure (QPP) for conducting commercial grade software evaluations, QPP 7.3, "Commercial Grade Software Evaluation" (Reference 52). The procedure provides a standard form as an attachment to capture the evaluation results. The items of information indicated by the form include safety function supported, functions provided by the item, failure modes, failure impact, critical characteristics, method of verification, and a tabular array for entry of each critical characteristic, acceptance criteria, and method of verification. The NRC staff reviewed the commercial grade software evaluation (CGSE) records for several of the software components as part of this SE (References 53 through 63). The findings of the critical design review and the evidence from verification activities are determined by the NRC staff to be acceptable based on the detailed evaluation documented in the following subsections. Consequently, the NRC staff concludes that HFC has followed the guidance of EPRI TR-106439 and, therefore, established dedication of the PDS of the HFC-6000 platform as acceptable for use in nuclear power plants. The CGD of the PDS is generic and not dependent on any specific application; therefore, this determination is suitable for reference when using the HFC-6000 platform for safety-related systems in nuclear power plants. Any maintenance modification of the dedicated PDS of the HFC-6000 platform must be treated according to the software QA plans as evaluated in Section 3.2.2 of this SE. Any new development of operating software intended for use in the HFC-6000 platform to support safety-related applications requires treatment under an acceptable software QA program.

3.2.1.1 Special Tests and Inspections

As part of the acceptance approach for CGD of digital equipment, EPRI TR-106439 identifies special tests and inspections as means to support verification of physical, performance, and dependability characteristics. In addition to referencing the CGD guidance in EPRI TR-106439, the EPRI TR-107330 guidance on generic qualification of PLCs for safety-related applications specifically identifies black box testing in Section 7.6.2 as one compensatory quality activity for legacy software to confirm conformance to its generic requirements. Code inspections, software object testing, software component testing, and functional testing are means of generating the compensatory evidence on critical design characteristics to confirm acceptable quality and performance in support of the CGD of PDS.

In Section 10.1.1.3 of the TR, HFC states that it performed supplemental testing of the PDS of the HFC-6000 platform to provide further evidence of product quality and establish its suitability to be dedicated for use in nuclear safety applications.
[

]

3.2.1.1.1 Source Code Inspection

To support the software dedication process, HFC performed a source code inspection of the predeveloped operating software, including the VHDL code of the onboard CPLDs. The stated objectives of this inspection were detection of specific types of faults, identification of any violations of HFC coding standards, and verification of the correctness of the code. Dependability characteristics reviewed as part of the code inspection include completeness, consistency, and validity. The static analysis of the code complemented the dynamic testing performed as part of the CGD process by identifying additional test cases to be considered. The findings also supplemented the commercial grade survey effort (see Section 3.2.1.2 of this SE) by contributing to the reconstitution of the design documentation of the PDS.

HFC established a work instruction (WI) for manual source code review to facilitate the inspection and ensure consistency among reviewers. Specifically, WI-ENG-830, "Source Code Review" (Reference 64), requires line-by-line code inspection by competent engineers that were not involved with the original design effort for the PDS to ensure compliance with the software requirements. As part of this inspection, every path must be traced through the program code, any calculation in the code must be verified to comply with the requirement, and any the operations represented by the code must be compared with those identified in the comments or associated documentation. The WI also requires that a system change request (SCR) be generated to address any discrepancy noted. A standardized review record form is provided to capture the review findings.

[

]

No other discrepancies from the source code inspection were reported in the TR. Thread audits conducted by the NRC staff during the on-site regulatory audits at the HFC facility also involved review of selected source code review records (References 15 and 16). Additionally, source code review records for VHDL logic were observed by the NRC staff in conjunction with thread traces that were conducted during the site visit in October 2009. The results from audits confirmed that the inspection findings were adequate to contribute to the dedication of the PDS of the HFC-6000. For example, potential unneeded code was identified in a sampled source code review record, which indicates the inspection was sufficiently detailed to adequately contribute to an assessment of the dependability characteristics of the PDS. In selected instances where an apparent discrepancy was noted in a record without corresponding information regarding how the discrepancy was resolved (e.g., an identified SCR), a condition report (CR) was generated and the resolution of the discrepancy was subsequently confirmed through the HFC corrective action program (Reference 67). Thus, based on the HFC docketed materials and confirmed by audit of the source code inspection records and the confirmation provided through the HFC corrective action process, the NRC staff determined that the code inspection findings are acceptable to support the dedication of the PDS of the HFC-6000 platform.

3.2.1.1.2 Application Software Object Tests

Section 5.6 of EPRI TR-107330 requires that application software object testing be conducted to supplement the software validation testing that should have been performed as part of the executive (i.e., operating) software development for a PLC platform. Application software objects are those software components that are provided as part of the platform software for use by (or in) application software.

To comply with the guidance in EPRI TR-107330 and support the CGD of the PDS of the HFC-6000 platform, application object testing was conducted on the HFC-6000 platform. As summarized in Section 10.1.3.1 of the TR, this testing included all software components that have a direct impact on the application code or that can be accessed by application code while it is being executed on the SYS processor of the HFC-SBC06 controller module. These software components are designated as application software objects (ASOs). The scope of the testing included both normal operations and exceptional conditions for the following ASOs:

[

]

The TR states that all ASO tests were completed and all acceptance criteria were met with no errors reported. The NRC staff reviewed selected test records during the on-site regulatory audits at the HFC facility as part of thread audits (References 15 and 16). An apparent anomaly was identified in the review of test records for an analog function block during the first audit but further inspection during the second audit, coupled with subsequent review of the test report (Reference 68), clarified the testing results and resolved the anomaly. Consequently, the NRC staff concurs that the ASO tests were successfully executed and finds that the ASO testing of the PDS of the HFC-6000 platform satisfies that requirement for such testing in EPRI TR-107330. In addition, the NRC staff concludes that the test results provide evidence of the performance and dependability characteristics of the ASO and are acceptable to support the dedication of the PDS of the HFC-6000.

3.2.1.1.3 Software Component Tests

As part of the testing activities to support the dedication of the PDS of the HFC-6000 platform, HFC conducted software component tests. HFC defines a software component as a set of self-contained software programs (e.g., software routine, function, task, operating system or sets of software files) that can be reused to build a software system. [

] These components are

maintained in the HFC software library and are typically installed in firmware for use in the various hardware modules of the HFC-6000 platform.

The software component testing performed by HFC is summarized in Section 10.1.3.2 of the TR. The comprehensive component test procedure developed by HFC is documented in TS001-000-01, "Component Test Procedure" (Reference 69). Software component tests were conducted on the specified software components that comprise the PDS of the HFC-6000 platform. Additionally, the hardware circuitry associated with each processor (e.g., board management CPLDs) was addressed under the scope of the test procedure. Software component testing activities included determining the features to be tested, designing test cases, designing the test set up and the test environment, identifying acceptance and rejection criteria, executing the tasks, analyzing test results, and reporting test findings. A test design is based on the software functions described in the software documentation of the PDS (see Section 3.2.1.2 and 3.2.3 of this SE) or the HFC-6000 product line requirement specification (Reference 19). Test inputs were defined during design of the test cases and the expected outputs were determined. Since the software components are part of the PCB firmware, the software component testing performed by HFC was mostly low level code testing using an emulator to create a simulation testing environment. Test software including one or more software components were executed through a single step process on a representative hardware platform. The test procedure specifies that component testing cover all routines and subroutines and that each program branch be exercised. The test outputs observed were compared against expected outputs so that any anomalies could be observed, recorded, and analyzed. The TR states in section 10.1.3.2 that all major software components were tested and no critical defects were detected. HFC defines a "critical software defect" as a defect in the basic system software that prevents the associated hardware module from processing inputs and obtaining correct actuation outputs. In effect, a critical defect could inhibit the execution of a safety function. For those non-critical defects that were detected and resolved, a regression test was performed with the modified version of the software component.

In addition to the review of the testing approach developed by HFC, the NRC staff inspected test records and processor-specific test procedures as part of thread audit activities during the on-site regulatory audits at the HFC facility (References 15 and 16). As part of a corrective action (Reference 70) to ensure completeness in the software requirements specification, HFC supplemented the operating system component testing by developing an addendum to the component test procedure (Reference 71). No anomalies with the test results were identified during the audits and the testing method was found to be appropriate. Thus, based on the review of the test procedures and confirmed by the audit of the component test records, the NRC staff finds that the software component testing results are acceptable to support the dedication of the PDS of the HFC-6000 platform.

3.2.1.1.4 Prototype and Functional Tests

Acceptable compensatory quality activities for legacy software are identified in Section 7.6.2 of EPRI TR-17330 and include black box testing that exercises software functions to confirm that performance requirements are satisfied. Functional testing provides a means to accomplish that objective while providing evidence that the performance and dependability characteristics of PDS are suitable for dedication to support safety-related applications. Additionally, EPRI TR-107330 also requires the execution of operability and prudency tests in Section 5.5 as part of the generic qualification testing of a PLC platform. These tests demonstrate the functional performance of the test specimen. The conduct of the operability and prudency tests is addressed in the evaluation of the qualification program for the HFC-6000 platform (see Section 3.3 of this SE).

The purpose of functional testing is to test the functionality of hardware modules and associated software components. To fulfill that purpose, HFC developed functional test procedures and acceptance criteria for the modules of the HFC-6000 platform based on the requirement specifications. Applying these procedures, HFC performed prototype and functional testing on the modules that comprise the HFC-6000 platform. This testing was performed with the final release version of software. The TR states that the functional test results show that all acceptance criteria are successfully met.

The NRC staff reviewed the prototype and functional test procedures that were docketed as a sample of the test methods. In particular, the procedures for the prototype tests for the HFC-SBC06 and HFC-DPM06 modules (Reference 72), the HFC-DC33 module (Reference 73), and the HFC-DO8J module (Reference 74) were reviewed along with the procedure for the functional test of the digital and analog I/O boards (Reference 39). The operability (Reference 76) and prudency (Reference 77) test procedures and results from the environmental qualification program for the HFC-6000 platform (see Section 3.3 of this SE) also were reviewed. Additionally, thread audits conducted by the NRC staff during the on-site regulatory audits at the HFC facility involved inspection of procedures and results for the prototype and functional tests (References 15 and 16). The test procedures and results that were inspected also addressed the board management functionality of the CPLDs either explicitly (e.g., the redundancy and failover mechanism) or implicitly through the execution of software dependent on the services provided by the CPLDs. No anomalies were found in the test results but an ambiguity in the test procedure for the HFC-SBC06 and HFC-DPM06 prototype test was identified. A condition report (Reference 78) was generated. The resolution of the CR led to the revision of the prototype test procedure and the issuance of an addendum to the operability test procedure (Reference 79) to ensure that the fulfillment of the software requirements is adequately confirmed by the test results. In addition, the prototype test for the HFC-SBC06 and HFC-DPM06 modules and the amended operability test procedure each include test coverage of the board management functionality provided by the onboard CPLDs. The review of the test procedures and the thread audit findings confirmed that the prototype and functional test results provide adequate indication of the suitability of the performance and dependability characteristics of the PDS. Thus, the NRC staff concludes that the testing approach and test findings are acceptable to support the dedication of the PDS of the HFC-6000 platform.

3.2.1.2 Commercial Grade Survey

As an element of the acceptance approach for CGD of digital equipment, EPRI TR-106439 identifies commercial grade surveys as means to support verification of dependability characteristics. Of the dependability characteristics, "built-in quality" addresses less quantifiable elements related to the development process and accompanying documentation. EPRI TR-106439 identifies review of vendor processes and documentation as a method of verification (associated with CGD Methods 2 or 3) for assessing the built-in quality. These processes and documentation include: (1) design, development, and verification processes, (2) QA program and practices, and (3) V&V program and practices. Acceptance criteria includes evidence that the vendor maintains a QA program that this generally in compliance with a recognized standard and that a process was used for legacy software which addresses essentially the same elements as the current QA process. The methods of verification include review of the evolution of vendor procedures and practices for software development, V&V, and testing as well as determination of the degree to which the QA program and software development process were applied. It is noted that preparation of supplemental documentation may be necessary.

In Section 10.1.1.4 of the TR, HFC states that the operating software in the HFC-6000 platform is COTS software developed for industrial, fossil power, and nuclear applications over time. The software QA approach for the heritage product lines utilized design, documentation, and testing practices common to the critical control industries at the time the software was developed. HFC also states that QA programs were applied during the development of the PDS software. In Reference 14, HFC discusses the QA processes in place during the development of the PDS. This information is summarized below.

The heritage of the HFC-6000 platform traces to two product lines developed by Forney Corporation beginning in the early 1980s. The operating software for the HFC-6000 platform is primarily derived from the ECS-1200 product line. From 1982 through the early 1990s, the basic features of the ECS-1200 product line were developed. [

]

In the late 1980s, Forney Corporation was engaged to supply a plant control system to the Yongwang nuclear power plant in South Korea. At that time, Forney Corporation developed a nuclear QA program based on the 1983 version of the American National Standards Institute/American Society of Mechanical Engineers (ANSI/ASME) standard for Nuclear QA Level 1 (NQA-1), "QA Program Requirements for Nuclear Facilities." Although the QA program of the Forney Corporation did not include a formal V&V process, the installation of the plant control system in 1994 at the plant in South Korea included post-delivery V&V of the design.

In mid-to-late 1990s, Forney Corporation achieved ISO 9000 certification for quality management and subsequent development of the heritage operating software occurred under that QA program. The Forney Corporation QA program adopted a life cycle approach that instituted many similar processes to those associated with a 10 CFR Part 50, Appendix B program. In 2000, Forney Corporation sold its product lines to Hunjung Heavy Industries (later Doosan Heavy Industries) and HFC was formed. As part of the transfer, HFC retained the ANSI/ASME NQA-1-based QA program and engineering procedures. Subsequently, the ECS-1200 product line was further developed and supplied to the Ulchin Nuclear Power Plant in South Korea as a plant control system. The HFC QA program evolved to support its acceptance as a nuclear-qualified supplier by Korea Hydro and Nuclear Company (KHNP), which is an international utility member of the Nuclear Procurement Issues Committee (NUPIC) organization. HFC has undergone quality audit in 2002 and 2007 by audit teams composed of representatives from KHNP, Korea Power Engineering Company (KOPEC), and Korea Institute of Nuclear Safety (KINS).

In the response to RAI Part 3 (Reference 17), HFC states that the five CPLDs from the HFC-SBC06 and HFC-DPM06 modules were treated exclusively as hardware following VHDL programming during their initial development. However, since the early 2000s, a development life cycle treatment was initiated, albeit without the availability of formal life cycle documentation. Consequently, the CPLDs were included as part of the dedication process for PDS. Following the dedication effort, HFC has confirmed that any subsequent modification to the VHDL code has been subject to the HFC software QA program (Reference 17).

The investigation of vendor processes in place throughout the product life cycle of the heritage product lines indicates that the PDS was subject to some QA processes that are compliant with a recognized standard during much of its development history. However, because life cycle V&V was not rigorously applied until later in its heritage, it cannot be claimed that the overall QA process employed in the main development activities for the PDS of the HFC-6000 platform addresses essentially the same elements as the current QA process. Thus, the commercial grade survey findings only partially support verification of the built-in quality characteristic. Consequently, the HFC software dedication program supplements the evidence with findings from special tests and inspections and performance records. The NRC staff concurs that the records of the original design and QA processes indicate favorable dependency characteristics and, when combined with findings from other verification methods, contributes to an acceptable determination of the suitability of the PDS to be dedicated for nuclear-safety applications.

As part of the CGD activities, HFC determined to reconstitute the software documentation for the operating software of the HFC-6000 because the original software documentation for the heritage product lines was incomplete and a review of the HFC-6000 platform documentation showed that improvements were required to demonstrate suitability for nuclear safety applications. Consequently, the software requirements and software design specifications for the HFC-6000 platform were generated. In particular, the module requirement specifications, module design descriptions, module detailed design specifications, and component specifications were updated. Additionally, software requirements for the predeveloped operating software were documented and requirements traceability matrix was generated to map requirements to implemented code and relevant documentation. The VHDL code for the onboard CPLDs was also addressed in the regenerated requirements, design, and traceability documentation. In Section 10.1.2.1 of the TR, HFC states that the reconstituted requirements specifications were written to follow current regulatory guidance. These documents and the compliance claims by HFC are evaluated in Sections 3.2.2.10.3 and 3.2.3 of this SE.

3.2.1.3 Performance Records

EPRI TR-106439 identifies review of product operating history as a method to support verification of the dependability characteristics of reliability and built-in quality as part of the acceptance approach for CDG of digital equipment. As part of the guidance on generic qualification of PLCs for safety-related applications given in EPRI TR-107330, the CGD guidance in EPRI TR-106439 is referenced as a source of acceptable compensatory quality activities for legacy software. Section 7.6.2 of EPRI TR-107330 also specifically identifies particular compensatory quality activities that include evaluation and analysis of documented operating experience for product revisions involving legacy software elements in similar applications, provided the revisions are under continuing configuration control.

In Section 10.1.1.4 of the TR, HFC claims that the operating history for the PDS of the HFC-6000 platform demonstrates sufficient built-in quality to be suitable for dedication for use in nuclear safety applications. Specifically, HFC notes that there is significant experience with the predeveloped operating software components in critical applications, including Korean nuclear power plants. Furthermore, HFC states that the software has been operating reliably for a long period of time with very few defects.

Section 10.1.4 of the TR describes a performance record evaluation of the PDS for the HFC-6000 platform. The assessment of software performance addresses relevant historical usage and involves determination of the hours of operation per software component type, the software defects that have been reported, the significance of the software defects, and the relevance of the defects for any nuclear safety application. The relevant performance records are based on the usage of the HFC product lines from which the operating software of the HFC-6000 was derived. Specifically, the operating histories of the ECS-1200 Plant Control System and AFS-1000 Boiler Safety and Nuclear Safety I&C System product lines are cited as applicable since the HFC-6000 platform incorporates the basic software components of these products. The AFS-1000 product is employed primarily for applications that provide single loop control of field equipment while the ECS-1200 product is employed primarily for multi-loop plant control system applications.

The relationship of the HFC-6000 platform to the AFS-1000 and ECS-1200 product lines is described in the TR. The IOMs for the HFC-6000 platform are direct adaptations (i.e., only form factor modifications) of AFS-1000 and ECS-1200 modules. Therefore, the IOM operating software for the HFC-6000 platform is identical to that of the predecessor product lines. The operating software for the HFC-6000 controller module (HFC-SBC06) is shown to be a subset of the software components for the AFS-1000 and ECS-1200 controller modules. Thus, the operating histories of the two predecessor product lines provide a suitable basis for establishing performance records to support the dedication of the PDS of the HFC-6000 platform. The assessment of those operating histories by HFC serves to indicate the quality and reliability of the predeveloped operating software employed by the HFC-6000 platform.

The TR states that the HFC-6000 and recent generation AFS-1000 operating software is essentially the same design with the exception of software differences arising from the use of different microprocessor versions. The earlier models of the AFS-1000 controller (i.e., SBC-01, SBC-02, and SBC-03) employ identical function logic and I/O software components while the later models (i.e., SBC-05, SBC-04N, and SBC-P04N) employ the same software components as the ECS-1200 product line and the HFC-6000 platform. In the TR, HFC summarizes the product line history for each model of the AFS-1000 by providing the model description and type, identifying the relevant software components, characterizing the nature of the general application field, and specifying the software features inherited by the HFC-6000 platform. It is shown that the AFS-1000 function logic and I/O circuitry are directly relevant to the dedication of HFC-6000 platform PDS. Of particular significance is the special I/O circuitry designed for the AFS-1000 to provide field device control specific to nuclear power applications (i.e., MOVs and electrically-operated breakers). Due to a common software configuration and operating system, the AFS-1000 operating history regarding other basic system software components is suitable to indicate the quality of the heritage of the predeveloped operating software components of the HFC-6000 platform. The TR notes that the AFS-1000 has been in use for extensive control applications at Units 3 and 4 of the Yongwang Nuclear Power Plant since 1994. No basic system software defects have been detected and no changes to the operating software have been required since delivery. The information documented on the operating history of the AFS-1000 provides qualitative evidence of built-in quality to support the CGD of the PDS for the HFC-6000 platform.

As stated in the TR, the operating software for the HFC-6000 platform is primarily based on that developed for the ECS-1200 product line (i.e., models ECS-02, ECS-03, ECS-04, and ECS-05) since 1982. The ECS-1200 product line was initially developed for industrial applications and evolved to its present version in 1996 as a suitable control system platform for nuclear power usage as well as for fossil power and industrial applications. The TR notes that the operating software version for each successive generation of the ECS-1200 more closely replicates the HFC-6000 platform software. Specifically, HFC summarizes the product line history for each model of the ECS-1200 by providing the model description and type, identifying the relevant software components, characterizing the nature of the general application field, and specifying the software features inherited by the HFC-6000 platform. This summary information establishes that the basic system software components dedicated for the HFC-6000 platform are a subset of those employed by the ECS-1200 product. [

] These software components of the ECS-1200 product are implemented in a common basic software configuration that is identical to that employed for the HFC-6000 platform. It is also noted that model ECS-05 provides relevant operating history experience for the hardware circuitry and processor-related service management logic to support implementation based on Intel Pentium processors. Thus, the software operating history of the ECS-1200 is directly applicable to the assessment of the dependability characteristics of the PDS of the HFC-6000 platform.

The treatment of the ECS-1200 operating history involved quantitative assessment of the usage experience for the PDS components. The TR identifies numerous key installations of various models of the ECS-1200 product line and emphasizes that model version ECS-05 was used to implement plant control at Units 5 and 6 of the Ulchin

Nuclear Power Plant in 2005 and 2006, respectively.[1] Considering this installed base for the ECS-1200, HFC calculated the total module operating years (TMOY) for each hardware module and the associated software components. The calculation of the TMOY for a module is based on the number of installations (i.e., plants), the number of instances of that module used for each specific installation, and the years of service for each installation. To ensure that these calculated values are representative of the PDS of the HFC-6000 platform, HFC grouped the installations by generation (i.e., model version) and only included the module operating years corresponding to a particular generation of ECS-1200 in the TMOY calculation for those specific software components that were identified as being common to the PDS of the HFC-6000 platform. For example, the module operating years for the ECS-05 generation was included in the calculations for each software component while the contribution from the generation corresponding to ECS-02 (pre-1986) only applied to the operating system, redundancy and failure mechanism, control algorithms, and software configuration components. [ ]

To support determination of the performance of the PDS components as demonstrated by historical usage, HFC identified the software defects that had been reported since 1995. Prior to 2000, defect tracking was accomplished primarily based on change orders and work orders for design changes under the control of the Forney Company. After August 2000, HFC implemented its configuration management and change control processes (see Section 3.2.2.11 of this SE) to track defects and determine whether a defect is a critical defect. [ ] The TR provides identification of each software defect, a description of the defect and the corrective action, an estimation of the defects per hour for each software component (based on the total operating hours from the ECS-1200 operating history), and a categorization of each defect as critical or non-critical.

Based on its analysis of the reported defects, HFC identified only one critical defect. This defect occurred with the controller supporting online monitoring by responding to peer-to-peer queries from an external workstation and corrective action was taken through a software revision.

HFC determined the defects per hour for the software components based on the calculated total operating hours and the reported defects. The defects per hour for those software components that had a reported defect range from 2.44×10^{-8} to 3.9×10^{-8}. HFC claims these results demonstrate excellent reliability for the software components. The NRC staff notes that only defects reported since 1995 are cited and the total operating hours since 1982 were used in the calculations. It is unclear whether data about defects prior to 1995 was maintained and considered in the analysis. Thus, the reliability results cannot be confirmed in this evaluation based on the available data. Nevertheless, the evidence presented by HFC does provide qualitative evidence to indicate the built-in quality and reliability of the PDS of the HFC-6000 platform.

---

[1] The installation at the Ulchin Nuclear Power Plant represents the earliest cited usage (Reference 17) for a subset of the board management CPLDs (i.e., PBUSIF and SBC6_CHSEL). Consequently, the CPLDs are not addressed in the operating history analysis.

The NRC staff reviewed the performance record evidence for PDS of the HFC-6000 platform that is documented in the TR and determined that it is adequate to contribute to CGD in accordance with the guidance in EPRI TR-106439 and EPRI TR-107330. HFC has established the relevance of the operating histories of the predecessor product lines to the operating software of the HFC-6000 platform and the cited performance indicates suitable dependability characteristics (i.e., built-in quality and reliability).

3.2.2 Life Cycle Planning Documentation

IEEE Std 603-1991 requires that the quality of components and modules be established and maintained in accordance with a QA program. IEEE Std 7-4.3.2-2003 amplifies this requirement in regard to software quality. SRP BTP 7-14 describes the basis for accepting software for safety functions as including confirmation that acceptable plans were prepared to control software development activities. Furthermore, SRP BTP 7-14, Section B.2.1, "Software Life Cycle Process Planning," identifies the software life cycle planning information subject to review in terms of the following documents:

- Software Management Plan
- Software Development Plan
- Software QA Plan
- Software Integration Plan
- Software Installation Plan
- Software Maintenance Plan
- Software Training Plan
- Software Operations Plan
- Software Safety Plan
- Software Verification and Validation Plan
- Software Configuration Management Plan

It is noted that the identified documents and organization of information constitute one representation of the required planning activities and other document structures can be equally valid.

The HFC QA Program Manual (QAPM) (Reference 80) defines the administrative measures and procedures necessary for assuring that all HFC hardware and software products satisfy project quality requirements and meet applicable industry codes and standards. The HFC QAPM addresses the organizational structure of the company, scope of the QA program, and control of designs, documents, items, processes and procedures, and tests, as well as providing requirements for test and inspection, corrective action, audits, and QA activities and documentation. A quality plan is developed for each specific project to define the particular QA activities to be performed in implementing the QA program.

As previously noted in Section 2.1 of this SE, the software included within the scope of the TR is composed of the predeveloped operating software of the HFC-6000 platform that has undergone CGD (see Section 3.2.1 of this SE). The treatment of new (e.g., application) software under the HFC software QA program is not addressed in this review. As identified in Section 2.1 and established in Section 5.2 of this SE, development of life cycle planning documentation for a specific safety-related system project is an ASAI and the HFC QA program for application software is subject to plant-specific review. Accordingly, the software life cycle processes and the associated plans and procedures established for the HFC-6000 platform were reviewed only to the extent to which they apply to the maintenance of the commercially dedicated PDS. Based on the evaluation documented below, the software life cycle planning documentation of the HFC QA program, as it relates to the maintenance of PDS, is acceptable for maintaining the validity of the commercial dedication.

Section 10.2 of the TR describes the HFC software QA program for the development of new software. In addition, the HFC response to RAI Part 3 (Reference 17) provides a mapping of the quality procedures and WIs to the planning documents identified in SRP BTP 7-14. However, as noted in the HFC response, several of these documents substantially relate to application-specific software development. Thus, since the identified QA plans discussed below include phases and activities that are specific to application software in whole or in part, some planning documents are either not relevant to the maintenance of the PDS software or cannot be fully evaluated solely in terms of the platform software. The subsections that follow address each of the life cycle planning documents that are identified in SRP BTP 7-14. The limitations of the extent of the review in the absence of a specific application are noted.

3.2.2.1 Software Management Plan

SRP BTP 7-14, Section B.3.1.1, “Acceptance Criteria for Software Management Plan (SMP),” provides acceptance criteria for SMPs. This section states that RG 1.173, “Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” endorses IEEE Std 1074-1995, “IEEE Standard for Developing Software Life Cycle Processes,” and that Clause A.1.2.7, “Plan Project Management,” of the standard contains an acceptable approach to software project management. Clause A.1.2.7 states that the plan should include planning for support, problem reporting, risk management, and retirement.

The purpose of the NRC staff review of a project management plan is to ensure that the management aspects of the corresponding development project demonstrate that high-quality programming will be the result of a deliberate, careful and high-quality development process.

As noted above, the HFC QAPM defines the administrative measures and procedures necessary for assuring that all HFC hardware and software products satisfy project quality requirements. For any specific project, development of a project management plan is required to identify the particular QA activities to be performed in implementing the QA program. The quality process procedure, QPP 1.2, “Organizational Responsibilities” (Reference 81), specifies the organizational structure and responsibilities that apply to product development and project performance while QPP 2.1, “Project Quality Plans” (Reference 82), defines the procedure for developing a project quality plan. A WI, WI-ENG-020, “Software Security” (Reference 83), serves to establish the software security aspects of the HFC development environment to contribute to risk management. Additionally, the HFC software safety plan, PP004-000-01, “Software Safety Plan” (Reference 84), defines the HFC approach to

3.2.2.8

managing software safety. Detailed evaluation of the plans and procedures for software safety and security are discussed in Sections 3.2.2.9 and 3.8, respectively, of this SE.

SRP BTP 7-14, Section B.3.1.10.4, "Review Guidance for the SVVP," identifies independence of the V&V organization as one of the most critical items in the SVVP. Consequently, it is significant that QA management and the provision of V&V oversight are the responsibility of a QA Department at HFC that is separate from the other departments responsible for a project (Reference 81). For each project, a QA manager is identified and a V&V team is specified. The QA manager is responsible for overseeing QA activities and the V&V team performs independent evaluation of the processes and products for a software life cycle implementation. QPP 2.1 includes a planning document template that facilitates ready identification of the applicable QA activities and methods and provides for reviews, holdpoints, audits, and corrective action.

The SMP for software implemented on the HFC-6000 platform is incorporated into a product/project development plan, which is application specific. As discussed in Sections 3.2.1 and 2.1 of this SE, the predeveloped operating software of the HFC-6000 platform is commercially dedicated. Consequently, a specific SMP addressing the PDS or its maintenance is not available. However, a product development plan (Reference 85) and a project quality plan (Reference 86) were generated for the ERD111 project on the generic qualification of the HFC-6000 platform. The product development plan addressed the effort to establish the HFC-6000 product line based on the technology from the previous HFC product lines. The items covered in the plan include project definition, organization responsibilities and assignments, project management activities for planning and execution, and project controls for deliverables, resource usage, QA, and risk assessment. The project quality plan primarily addressed the development of the test specimen for environmental qualification testing so it is not directly related to the management of the PDS. Nevertheless, the plan for the ERD111 project illustrates the application of the QA program and associated procedures and, in the case of the product development plan, governed the inspection, testing, and documentation activities to support the CGD of the PDS.

The elements of a software management plan to support maintenance of the PDS of the HFC-6000 platform are provided by the cited documents (References 80, 81, 82, 83, and 84). Based on evaluation of these procedures and the example provided by the ERD111 plans, the NRC staff finds acceptable provisions in place to establish adequate oversight, control, reporting, review, and assessment for the PDS.

3.2.2.2 Software Development Plan

The acceptance criteria for a software development plan (SDP) are contained in SRP BTP 7-14, Section B.3.1.2, "Software Development Plan (SDP)." This section states that RG 1.173 endorses IEEE Std 1074-1995, subject to exceptions listed, as providing an approach acceptable to the NRC staff for meeting the regulatory requirements and guidance as they apply to development processes for safety system software. The section also states that Clause 5.3.1, "Software Deployment," of IEEE Std 7-4.3.2-2003 contains additional guidance on software development.

The NRC staff review of the software development is primarily intended to determine that use of the SDP results in a careful, deliberate and high-quality development process that will result in high-quality programming, suitable for use in safety-related systems in nuclear power plants. While many of the details on how this will be performed may be found in other plans, the important aspect of the SDP is the method to be used to make sure these other plans are being applied. This includes a provision for effective oversight to monitor the software development process, and to consider risk associated with the size and complexity of the product.

The SDP should clearly state which tasks are a part of each life cycle phase, and identify the life cycle inputs and outputs. The review and V&V of those outputs should be defined. The methods and tools to be used during the development process should be evaluated, as well as the method used to detect defects produced through the use of those methods and tools.

The HFC software QA program provides a process procedure defining the software life cycle and establishing the V&V program. This procedure, QPP 3.2, " Software Life Cycle and Verification/Validation Program" (Reference 87), specifies development of a master schedule with V&V activities keyed to life cycle phases, which are defined to be consistent with the life cycle processes identified in IEEE Std 1074-1995 and IEEE Std 1012-1998, "IEEE Standard for Software Verification and Validation." The HFC software life cycle model consists of the following phases: planning, requirements, design, implementation, component integration, integration/acceptance test, installation and checkout, operation and maintenance, and retirement. It is noted in the procedure that HFC distinguishes between product development and an application project. Tasks for V&V at each life cycle phase are identified for each type of project and the corresponding life cycle inputs and outputs are specified. Methods and tools for conducting V&V activities are identified in the procedure. Software development tools are identified in development plans for specific projects, such as VV0401, "Product Development Plan" (Reference 85), from the ERD111 project for the generic qualification of the HFC-6000 product line. The development tools are maintained under configuration control and the software products generated by their use are subjected to the full range of V&V activities, such as inspections and tests, that are prescribed by the software life cycle procedure (Reference 87) and the associated V&V WI (Reference 88).

As is the case for the SMP discussed above, the SDP for software implemented on the HFC-6000 platform is incorporated into an application- or project-specific development plan. Development of application software for a plant-specific implementation of the HFC-6000 platform is outside the scope of this review, so the evaluation of software development plans is focused on the platform operating software. Since the commercially dedicated operating software of the HFC-6000 platform was developed prior to the establishment of the HFC software QA program, a specific SDP addressing the PDS or its maintenance is not available. Nevertheless, the SDP for the ERD111 project illustrates the approach to project planning associated with product development (i.e., a nuclear qualified HFC-6000 platform). This SDP demonstrates provisions for effective oversight and execution of a project that would be relevant to software maintenance activities as part of further development of the HFC-6000 product line.

The elements of a SDP to support maintenance of the PDS of the HFC-6000 platform are provided by the procedure for establishing software life cycle plans and illustrated by the example of the ERD111 plan. Based on the review of the cited documents, the NRC staff has determined that the procedures for establishing a SDP exhibit the management, implementation, and resource characteristics identified in SRP BTP 7-14 and are, therefore, acceptable for the maintenance of the PDS.

3.2.2.3 Software QA Plan

QA is required by 10 CFR Part 50, Appendix B, and the Software QA Plan (SQAP) should be implemented under an NRC-approved QA program. The regulation at 10 CFR Part 50, Appendix B, allows the licensee to delegate the work of establishing and executing the QA program, but the licensee shall retain responsibility. The SQAP should identify which QA procedures are applicable to specific programming processes, and identify particular methods chosen to implement QA procedural requirements. There are several RGs and standards that offer guidance.

1. RG 1.28, Revision 3, "QA Program Requirements (Design and Construction)," that endorses ANSI/ASME NQA-1-1983 and the ANSI/ASME NQA-1a-1983 Addenda, "Addenda to ANSI/ASME NQA-1-1983, 'QA Program Requirements for Nuclear Facilities'."

2. RG 1.152, Revision 2, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," endorses IEEE Std 7-4.3.2-2003.

3. RG 1.173 endorses IEEE Std 1074-1995.

4. NUREG/CR-6101, "Software Reliability and Safety in Nuclear Reactor Protection Systems," Section 3.1.2, "Software QA Plan," and Section 4.1.2, "Software QA Plan," contain guidance on these plans.

The NRC staff review of QA plans is required to determine that the plan exhibits the appropriate management, implementation, and resource characteristics as discussed in the SRP BTP 7-14, Section B.3.1.3, "Software QA Plan (SQAP)," and that use of the plan will result in high-quality software that will perform the intended safety function.

The HFC QAPM defines the QA program for HFC products and their constituent hardware and software components. It is designed to comply with ANSI/ASME NQA-1-2004, "QA Requirements for Nuclear Facility Applications," as well as 10 CFR Part 50, Appendix B. The HFC QA program is implemented through quality procedures, quality plans, WIs, and process control sheets. QA forms are used to capture objective evidence to demonstrate effective implementation. The HFC SQAP is embodied within the QAPM. Its provisions are realized in project-specific management plans for product or system development.

Specific elements of the QAPM address organization, the scope and management of the QA program, requirements and mechanisms for control of products, resources and processes, provisions for inspections, audits, and corrective actions. Each element of the QAPM identifies the implementing procedures, which in turn establish the basis for planning and execution of QA activities, provide forms and checklists, and identify relevant WIs. Specifically, as discussed in Section 3.2.2.1 of this SE, QPP 2.1 defines the procedure for identification of the applicable QA activities and provides for reviews, audits, and corrective action. For each application or product development project, a specific quality plan is developed as part of the project management plans in accordance with the QAPM based on the process defined in QPP 2.1. Additionally, QPP 3.2 defines the software life cycle model applied to software development planning to promote a high quality process and ensure the quality of the resultant software product. Sections 3.2.2.2 and 3.2.2.10.1 of this SE discuss the provisions of QPP 3.2 for development of a master schedule with V&V activities keyed to life cycle phases.

A separate QA Department is provided by HFC to promote independence of QA activities from development activities and the QA Director has stop work authority. Periodic audits of the QA program and project tasks are required. It is specified that these audits are to be conducted by qualified personnel independent of those having direct responsibility for the activity being audited. A corrective action program is specified to report and resolve any identified conditions adverse to quality. Software V&V and software configuration management are addressed in more detail in Sections 3.2.2.10 and 3.2.2.11, respectively, of this SE.

The QAPM and its associated quality process procedures provide measures to ensure that software maintenance activities for the PDS of the HFC-6000 platform maintain the acceptable quality demonstrated through the CGD effort. Based on the review of the QA processes and procedures identified in the QAPM, the NRC staff has determined that the manual and the associated quality procedures are appropriate for maintaining the suitability of the PDS for use in safety-related systems in nuclear power plants.

3.2.2.4 Software Integration Plan

The acceptance criteria for a software integration plan (SIntP) are contained in SRP BTP 7-14, Section B.3.1.4, "Software Integration Plan." This section states that RG 1.173 endorses IEEE Std 1074-1995 and that within that standard, Clause A.1.2.8, "Plan Integration," contains an acceptable approach related to planning for integration. Clause A.1.2.8 states that the software requirements and the software detailed design should be analyzed to determine the order for combining software components into an overall system, and that the integration methods should be documented. The integration plan should be coordinated with the test plan. The integration plan should also include the tools, techniques, and methodologies needed to perform the integrations. The planning must include developing schedules, estimating resources, identifying special resources, staffing, and establishing exit or acceptance criteria.

NUREG/CR-6101, Section 3.1.7, "Software Integration Plan," and Section 4.1.7, "Software Integration Plan," provide additional guidance on software integration plans. Section 3.1.7 states that software integration actually consists of three major phases: integrating the various software modules together to form single programs, integrating the result of this with the hardware and instrumentation, and testing the resulting integrated product. It further states that during the first phase, the various object modules are combined to produce executable programs. The second phase is when these programs are then loaded into test systems that are constructed to be as nearly identical as possible to the ultimate target systems, including computers, communications systems, and instrumentation. The final phase consists of testing the results, and is discussed in another report.

The integration activities noted above primarily relate to the applied product, in which the application software integrates the basic functionality of the operating software into programs that are then executed within the operating environment of the platform. Thus, plans for this aspect of software integration are application specific and cannot be evaluated at the platform level. Since the operating software for specific processors of the HFC-6000 platform is implemented as embedded firmware burned onto dedicated PROMs that are installed onto PCBs, the commercially dedicated PDS is intrinsically integrated with the hardware. Consequently, an integration plan for the operating software of the platform is not needed. Therefore, the SIntP is not applicable to the maintenance of PDS of the HFC-6000 and no evaluation was required.

3.2.2.5 Software Installation Plan

The acceptance criteria for a software installation plan (SInstP) are contained in SRP BTP 7-14, Section B.3.1.5, "Software Installation Plan." This section states that RG 1.173 endorses IEEE Std 1074-1995 and that Clause A.1.2.4 of that standard, "Plan Installation," contains an acceptable approach relating to planning for installation. This clause states that an installation plan describes the tasks to be performed during installation, and shall include the required hardware and other constraints, detailed instructions for the installer, and any additional steps that are required prior to the operation of the system. Further guidance is provided in NUREG/CR-6101, Section 3.1.8, "Software Installation Plan," and Section 4.1.8, "Software Installation Plan," that contains a sample outline of an installation plan.

The installation characteristics identified in the cited guidance generally apply to application software and its integration into an operating environment rather than to the basic embedded operating software of the HFC-6000 platform, which is installed as dedicated PROMS onto PCBs. Thus, the SInstP is an ASAI.

3.2.2.6 Software Maintenance Plan

The acceptance criteria for a software maintenance plan (SMaintP) are contained in SRP BTP 7-14, Section B.3.1.6, "Software Maintenance Plan (SMaintP)." This section states that NUREG/CR-6101, Section 3.1.9, "Software Maintenance Plan," and Section 4.1.9, "Software Maintenance Plan," contain guidance on software maintenance plans. These sections break the maintenance into three activities: failure reporting, fault correction, and re-release procedures. SRP BTP 7-14, Section B.3.1.6 further states that guidance on maintenance and configuration management of commercially dedicated items can be found in IEEE Std 7-4.3.2-2003, Clause 5.4.2.3, "Maintenance of Commercial Dedication." Additionally, EPRI TR 106439, Section 5, "Maintenance of a Commercial Dedication," provides guidance addressing the need for adequate configuration control and change management to maintain the validity of a commercial grade item dedication. In the guidance, maintenance of the dedicated item and the impact of product changes, including software revisions, are covered.

IEEE 1074-1995 describes maintenance as a post-development process in the general software life cycle model. SRP BTP 7-14 illustrates a representative software life cycle with operations and maintenance activities grouped together. Consequently, maintenance planning often focuses on maintaining applied software following installation. As identified in Section 2.1 of this SE, treatment of application software under the HFC software QA program is outside the scope of this evaluation. Since no specific application project has been established, a standalone SMaintP is not available. Nevertheless, configuration control is a key dependability characteristic of digital equipment and is required to maintain the dedication of a commercial grade item. Consequently, evaluation of the software maintenance process and procedures is essential to having confidence that the HFC software QA program can ensure the continued integrity of the CGD of the PDS of the HFC-6000 platform.

As described in Section 10.1.5 of the TR, software corrective action and configuration management procedures and WIs, under the software life cycle model defined in QPP 3.2, govern the maintenance of the operating software for the HFC-6000 platform. Specifically, QPP 16.1, "Corrective Action Program" (Reference 89), and WI-ENG-003, "Configuration Management" (Reference 90), provide the relevant procedures, activities, and methods that are applicable to the maintenance of PDS. The Corrective Action Program (CAP) provides for nonconformance reporting and correction while the change control process for configuration management provides an authorization structure and control mechanisms for items (e.g., code, documents) affected by the corrective action. The HFC CAP defined in QPP 16.1 is initiated whenever an error, non-conformance status, or condition adverse to quality is discovered. In addition to invoking the CAP, Section 8.5.5 of the TR further states that HFC is committed to comply with 10 CFR Part 21 in fulfilling its responsibility as manufacturer and dedicator of the HFC-6000 platform. To facilitate discharge of this responsibility, HFC has established a procedure for complying with 10 CFR Part 21 through identification and reporting of defects and nonconformance (Reference 91).

As a means to initiate the corrective action process, the CAP provides a CR template for initial documentation of any detected error or deficiency. The CR is entered into a change management software tool, the Serena Software Polytron Version Control System (PVCS) Tracker, provided as part of the configuration management system. This tool enables automatic resolution tracking and facilitates notification, review, and approval. A Condition Review Group (CRG) reviews the CR, determines its significance, and directs the assignment of responsible personnel. The CRG is a management group consisting of, as a minimum, the project manager, a QA manager, Director of Operations, and applicable engineering managers. Subsequent activities under the CAP involve investigation/analysis of the issue, determination of a corrective action to resolve the issue, evaluation and approval of the plan for corrective action, and implementation of the corrective action. Closure of the CR involves documentation of the implementation of the corrective action on a template provided by QPP 16.1.

For each item under software configuration management control, a person is identified as the owner of the item and has the responsibility to create, maintain, and manage changes to the component. When modification of the PDS is required by a corrective action plan, the HFC configuration management process provides mechanisms for the initiation, review, and approval of an SCR using the PVCS Tracker tool. The software owner performs an impact analysis and requests implementation approval from a Software Management Team (SMT), whose members include the Engineering Director, QA manager, and V&V team leader. The software components of the HFC-6000 platform are version controlled and subject to the change control process in accordance with WI-ENG-003. Librarian software (Microsoft Visual SourceSafe) makes available a working copy of the software code for a new project to execute the modification only when an individual has appropriate authorization granted by the SMT. The owner of the software is responsible for implementation of the change under the HFC software QA program. A software V&V team is specified as participants in the approval, life cycle activity, and signoff for SCRs involving software. The software life cycle and V&V procedure, QPP 3.2, specifies validation activities (e.g., regression testing) to ensure a change or corrective action does not introduce new hazards or anomalies.

Management review and ownership authority are administrative mechanisms employed to oversee and control change requests and corrective actions. The PVCS Tracker tool supports implementation signoff following execution of the change. The participation of the QA manager and V&V team in the implementation of software changes under the CAP promote adherence to quality processes and procedures. On closeout of an SCR, the modified software is registered into the software library as a new release with unique project and part number identification.

The TR and the software V&V report for the ERD111 project, VV0415, provide examples of software maintenance that occurred during the dedication of the operating software and following the generic qualification of the HFC-6000 platform. As documented in Sections 10.1.2.4 and 10.1.3.2 of the TR and noted in Section 3.2.1.1.1 of this SE, HFC dedication efforts included code inspections and component tests that identified a few code discrepancies. As stated in the TR, further analysis and regression test results validate that these discrepancies were addressed successfully through the CAP. Another example of maintenance for the PDS during the dedication and qualification effort arose when test results from environmental qualification testing of the HFC-6000 test specimen indicated the need for modifications to hardware and operating software parameters to resolve inadequacies in the performance envelope for the HFC-6000 product line (Reference 92). Specifically, a hardware reconfiguration was performed for the hardware watchdog timer of the controller module, a software parameter change was affected for the software watchdog timers of the controller module, and hardware and software changes were accomplished for the analog input module (References 66 and 93). [

] Regression testing validated the implementation of the maintenance changes.

The CAP and configuration management process contained within QPP 16.1 and WI-ENG-003, respectively, provide measures to ensure that software maintenance activities for the PDS of the HFC-6000 platform maintain the acceptable quality demonstrated through the CGD effort. Specifically, the CAP provides for fault reporting and fault correction. The configuration management process for change control contributes to fault correction by providing an authorization structure and resolution tracking mechanisms. The configuration control mechanisms for software items provide adequate re-release procedures for software that has undergone change as part of maintenance. Based on a review of the cited procedures and consideration of the software maintenance examples from the dedication and qualification of the HFC-6000 platform, the NRC staff has determined that the CAP and configuration management process exhibit the management, implementation, and resource characteristics identified in SRP BTP 7-14 and comply with the guidance on maintenance of a commercial dedication provided by EPRI TR-106439. Therefore, the CAP and configuration management procedures are acceptable as the basis for a maintenance plan to preserve the suitability of the PDS for use in safety-related systems in nuclear power plants.

3.2.2.7 Software Training Plan

The acceptance criteria for a software training plan (STrngP) are contained in SRP BTP 7-14, Section B.3.1.7, "Software Training Plan." This section states that RG 1.173 endorses IEEE Std 1074-1995 and that Clause A.1.2.6 of that standard, "Plan Training," contains an acceptable approach relating to planning for training. SRP BTP 7-14, Section B.3.1.7 also states that NUREG/CR-6101, Section 3.1.10, "Software Training Plan," contains further guidance on software training plans.

Clause A.1.2.6 of IEEE Std 1074 requires different types of training depending on the need. It states that training tools, techniques, and methodologies shall be specified, and that the planning shall include developing schedules, estimating resources, identifying special resources and staffing, and establishing exit or acceptance criteria. This planning shall be documented in the training planned information.

SRP BTP 7-14, Section B.3.1.7 further points out that the training plan may be quite simple or very complex, depending on whether the vendor or the licensee is doing the maintenance. The section states that if the licensee has contracted with the vendor to perform the maintenance, the licensee personnel only need to know how to operate the digital equipment, and this is typically less complex than the knowledge required to maintain the equipment. The review guidance also points to an intermediate step, where the licensee personnel perform first level maintenance, determining which sub-unit, such as an individual printed circuit board, is failed, replacing that sub-unit, and then sending the unit to the vendor for repair.

The training characteristics identified in the cited guidance primarily address user training for system maintenance and other user interactions related to application software. HFC maintains control of the operating software of the HFC-6000 platform and the embedded software on the installed PROMs cannot be modified in the field. Thus, the STrngP is not applicable to the PDS of the HFC-6000 platform and no evaluation was required.

3.2.2.8 Software Operations Plan

The acceptance criteria for a software operations plan (SOP) are contained in SRP BTP 7-14, Section B.3.1.8, "Software Operations Plan." This section states that the primary aspect for consideration is completeness. However, it adds that the operations plan needs to address the security of the system. In particular, the plan should identify the means used to ensure that there are no unauthorized changes to hardware, software and system parameters, and that there is monitoring to detect penetration or attempted penetration of the system.

Because the operation of a safety-related system is a licensee, and not a vendor, responsibility, there is no requirement for the vendor to have an operations plan and no evaluation was required. Features of the HFC-6000 platform that may assist licensees in establishing a secure operational environment are addressed in Section 3.8.

3.2.2.9 Software Safety Plan

The acceptance criteria for a software safety plan (SSP) are contained in SRP BTP 7-14, Section B.3.1.9, "Software Safety Plan (SSP)" and Section B.3.2.1, "Acceptance Criteria for Safety Analysis Activities." These sections state that the SSP should provide a general description of the software safety effort, and the intended interactions between the software safety organization and the general system safety organization. It further states that NUREG/CR-6101, Section 3.1.5, "Software Safety Plan," and Section 4.1.5, "Software Safety Plan," contain guidance on SSPs. RG 1.173, Section C.3, "Software Safety Analyses," contains guidance on safety analysis activities while NUREG/CR-6101 also addresses guidance for these analyses.

HFC has developed PP004-000-01 (Reference 84) as its SSP. The plan defines additional reviews, analyses, and evaluations to be included in the software V&V activities to ensure safety is addressed in the design and development of a safety-related system. The Director of Engineering has authority over the generation and implementation of a project-specific SSP. Although HFC does not have a dedicated software safety team and there is not a specific individual dedicated as a safety officer, the responsibility for ensuring that software safety concerns are adequately addressed is assigned to the project manager. In addition, organizational roles and responsibilities for software safety within the framework of a development project are delineated in the HFC SSP. While the QA manager retains responsibility for ensuring safety documents are maintained and controlled as part of the project-specific Quality Verification Data List (QVDL), it is the V&V team that is charged with executing and/or overseeing additional activities focused on software safety. In particular, a software hazard analysis (SHA) is required for both application and operating software and software safety analyses are mandated at the completion of each life cycle phase for a safety-related software component.

The safety analyses specified in the SSP include requirements analysis, design analysis, code analysis, safety test analysis, and change analysis. The HFC SSP differentiates between application and operating software, with the safety analysis activities described in terms of each type of software. The software safety requirements analysis for existing modules focuses on identifying any necessary hardware/software development and determining means, such as existing or new platform safety design characteristics or system architectural approaches, to mitigate the applicable abnormal conditions and events (ACE) identified in the SHA. The software safety design analysis for operating software addresses the functionality provided by the platform and considers the safety design characteristics that have been incorporated into the PDS. The software safety code analysis for existing modules addresses traceability, internal logic, interface (i.e., communication) support, and coding style (i.e., compliance with specified HFC coding practices) while the software safety test analysis encompasses component and module testing as well as system integration and functional testing. The software safety change analysis involves assessment of the safety impact of changes to existing modules or the design for the system under development. Regarding VHDL code, the SSP states that safety design considerations (e.g., potential failure modes) for CPLDs are addressed as part of the hardware failure modes and effects analysis but the code development is subject to the HFC software V&V program.

The HFC SSP notes that predeveloped operating software, which is implemented as firmware, does have the potential to impact the execution of safety-related application software. Thus, an evaluation of the PDS as an existing design is specified in the SSP. The starting point is identified as the existing design and test documentation for the PDS. As noted above, the existing PDS capabilities are evaluated for each project to identify the need for and scope of any software development. Generic hazard and safety analyses have been performed at the module level for the HFC-6000 platform. The results of these analyses are documented in the requirements and module design specifications that were reconstituted as part of the CGD of the PDS for the HFC-6000 platform (see Sections 3.2.1 and 3.2.3 of this SE). The initial submitted version of the reconstituted requirements specification for the operating software, Revision A of RR901-000-37, "HFC-6000 Controller SC, SAP, SEP Firmware Requirement Specification" (Reference 94), and the IOM requirements specification, 700901-6, "General I/O Cards Requirements Specification" (Reference 95), document findings from module level safety analyses for the PDS. The requirements specifications describe the criticality to safety of software components and identify hazard, security, and risk findings. The module specification for the controller firmware, MS901-000-01 (Reference 30) documents design features for the controller module that mitigate the identified hazards and risks as well as addressing means to support security. Additionally, RR901-000-23, "HFC Safety Control System Security Concept" (Reference 28), documents a conceptual phase assessment conducted to identify potential security vulnerabilities of the HFC-6000 platform.

Other specified safety analysis and testing activities have been executed for the PDS of the HFC-6000 platform. Source code inspections were performed and documented for the PDS as part of the dedication effort (see Section 3.2.1.1.1 of this SE). Additionally, extensive testing of the PDS, from structural tests through software component tests, was completed to support dedication, with the official record of the test results retained (see Sections 3.2.1.1.2, 3.2.1.1.3, and 3.2.1.1.4 of this SE). For modified software, the SSP specifies a software safety change analysis as well as development and execution of new component tests and regression tests to demonstrate the performance and safety of the modified module. However, any modification of the PDS beyond maintenance is considered to be new software development and its treatment under the HFC software QA program is outside the scope of this review.

Based on a review of the HFC SSP, the safety analysis findings and safety design characteristics described in the software documentation, and the testing and inspection evidence generated as part of the dedication effort for the PDS of the HFC-6000 platform, the NRC staff finds that the generic safety analysis results demonstrate the suitability of the PDS for safety-related use at nuclear power plants. Further, the analysis and testing findings for the PDS are appropriate for use as input to application-specific hazard and safety analyses.

The HFC SSP requires that all PDS be included in the SHA and addressed in life cycle safety analyses for a project. This requirement involves further evaluation of the PDS against the specific requirements of the application to determine whether the operating software functionality and safety design are adequate for a plant-specific system. As noted above, the generic safety analysis findings previously developed for the PDS of the HFC-6000 platform are suitable as input for project-specific analyses but adherence to the SSP requires further assessment within a system context throughout the software life cycle. Where modification of the PDS is required to maintain its performance or repair nonconforming items, the NRC staff finds the provisions for software safety change analysis identified in the HFC SSP to be adequate. Based on the review of PP004-000-01, the NRC staff has determined that the software safety activities defined for treating predeveloped operating software exhibit the management, implementation, and resource characteristics identified in SRP BTP 7-14 and are, therefore, acceptable for the maintenance of the PDS.

3.2.2.10 Verification and Validation

Verification is defined as the process of determining whether the products of a given phase of the development cycle fulfill the requirements established during the previous phase. Validation is defined as the test and evaluation of the integrated computer system to ensure compliance with the functional, performance, and interface requirements. Combined, V&V is the process of determining whether the requirements for a system or component are complete and correct, the products of each development phase fulfill (i.e., implements) the requirements to meet the criteria imposed by the previous phase, and the final system or component complies with specified requirements. This determination may include analysis, evaluation, review, inspection, assessment, and testing of products and processes.

Planning for the V&V enables up front identification of all necessary V&V tasks and promotes effective implementation of the embedded V&V process throughout the life cycle of safety-related software. Products of the V&V activities demonstrate that the plans have been successfully executed. Although the commercially dedicated operating software of the HFC-6000 platform was not developed under the HFC software QA program, the evaluation of the constituent software V&V plan that is described below enables a determination by the NRC staff that the V&V plan with its associated processes and procedures are acceptable for the maintenance of the PDS and are adequate to preserve its dedication. In addition, specific V&V products associated with the dedication activities for the operating software and the effort to generically qualify the platform have been docketed by HFC or were subject to review during the on-site regulatory audits at the HFC facility (References 15 and 16). As discussed below, the review of those V&V products supports a determination by the NRC staff that the HFC-6000 platform is suitable for safety-related use at nuclear power plants.

3.2.2.10.1 Software Verification and Validation Plans

The acceptance criteria for software V&V plans (SVVPs) are contained in SRP BTP 7-14, Section B.3.1.10, "Software V&V Plan (SVVP)." This section states that RG 1.168, Revision 1, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," endorses IEEE Std 1012-1998, "IEEE Standard for Software Verification and Validation," as providing methods acceptable to the NRC staff for meeting the regulatory requirements as they apply to V&V of safety system software. This section also states that further guidance can be found in RG 1.152, Revision 2, Section C.2.2.1, "System Features," and NUREG/CR-6101, Sections 3.1.4, "Software Verification and Validation Plan," and 4.1.4. "Software Verification and Validation Plan."

One of the required attributes of V&V is independence. RG 1.168 states that the organization performing the V&V tasks have financial, managerial, and technical independence; however, the NRC staff position is that this does not necessarily mean that a separate company should perform independent V&V. RG 1.168 also states that software used in nuclear power plant safety systems should be assigned integrity level 4 as defined by IEEE Std 1012-1998.

As noted in Section 3.2.2.1 of this SE, the organization structure at HFC described in QPP 1.2 includes separate departments for engineering and QA. The Engineering Department has responsibility for execution of a project, including software development, while the independent QA Department is responsible for execution of the QA program, including document control and establishment of a V&V team. As specified in the V&V procedure, QPP 3.2, and clarified in the HFC response to RAI Part 3 (Reference 17), a QA manager is identified for each project and a separate V&V team leader is assigned. Each of these key personnel reports independently to the HFC Director of Quality, who reports directly to the President of HFC (Reference 87). The degree of independence required between the V&V team and project team depends on the class of software. HFC classifies four levels of software (protection, important-to-safety, important-to-availability, and general), which correspond to the four categories defined in IEEE 1012-1998 (high, major, moderate, and low). The software of the HFC-6000 platform is treated as protection class software. Therefore, the V&V team leader is drawn from the QA Department to ensure administrative and financial independence from the project manager and Engineering Department. Team members are selected based on needed technical knowledge and skills but they are administratively prohibited from having past or current involvement in the development activities for the project. The NRC staff finds that the HFC approach to independence of V&V for the HFC-6000 platform complies with the guidance of IEEE Std 1012-1998 as endorsed by RG 1.168 and is, therefore, acceptable.

Since the commercially dedicated PDS of the HFC-6000 platform was developed prior to the institution of the HFC software QA program, a specific SVVP addressing the PDS or its maintenance is not available. The basis for an SVVP is found in QPP 3.2, WI-ENG-022, and PP901-000-04. These procedures and WIs incorporate verification reviews and validation testing within the V&V program. QPP 3.2 defines the life cycle for the development and maintenance of software and establishes the software V&V program to be applied for each software project. Within the procedure, organizational responsibilities are identified; a master schedule is established based on the defined life cycle, V&V roles for key project assignments are listed, tools and methodologies are identified, and V&V tasks are specified, including methods (i.e., procedures and WIs), inputs and outputs, and documentation requirements. WI-ENG-022, "Software Verification and Validation" (Reference 88), provides the specific requirements for the V&V process applied to a project from initial planning through the completion of acceptance testing. The HFC SSP, PP004-000-01, defines specific V&V responsibilities and activities (e.g., safety analyses) to address software safety. These provisions are discussed in Section 3.2.2.9 of this SE. Regarding CPLDs, the SSP and the HFC response to RAI Part 3 (Reference 17) establish the position that the software V&V procedures and software life cycle approach for the HFC software QA program apply to the development and maintenance of VHDL logic code.

QPP 3.2 specifies verification reviews at each phase of the software life cycle. These reviews are supported by the use of checklists, which are provided as part of WI-ENG-022, and requirements traceability analyses. A requirements traceability matrix (RTM) serves as the vehicle for capturing the verified traceability throughout the life cycle. Other analyses that are identified in the procedure include failure modes and effects analysis, reliability analysis, and hazard analysis. Furthermore, WI-ENG-022 specifically requires that criticality, hazard, security, and risk analyses be conducted as part of every life cycle phase. In addition, PP901-000-04 specifies safety analyses at each phase of the software life cycle and, in particular, identifies assessment of requirements in terms of reliability and security. The CAP, which is discussed in Section 3.2.2.6 of this SE, is identified as the method for reporting and tracking any condition adverse to quality.

Validation testing is also specified in QPP 3.2 and WI-ENG-022. These tests include software component testing, prototype testing of modules, qualification testing of applications, and acceptance testing of systems. Section 3.2.2.12 of this SE documents the review of these provisions.

Reporting requirements for software V&V activities are specified in QPP 3.2. These reports include task reports documenting each review, test, or analysis at every life cycle phase and cumulative analysis reports addressing analyses and testing such as qualification, system availability, identification and mitigation of ACEs, and failure modes and effects. A comprehensive system V&V report is required to describe the V&V activities and findings, summarized on a phase-by-phase basis, throughout the project life cycle. This SE is intended to provide objective evidence of the oversight and assessment conducted during the course of the project.

QPP 3.1, "Design Control" (Reference 96), requires a repeated verification effort for changes to a previously verified design, including an impact analysis. QPP 3.2 provides administrative procedures for CR resolution and V&V task iteration to ensure quality processes are invoked for software maintenance. Specifically, the procedure and associated WI identify the need to perform regression testing for modified software. In addition, the SSP specifies conduct of a software change analysis for modification of existing software.

The basis for software V&V planning is contained in QPP 3.2, WI-ENG-022, and PP004-000-01. These processes, procedures, and plans provide for development of a suitable program with specified V&V tasks integrated into the life cycle phases for a software project. The specification of organizational responsibilities, determination of methods, identification of V&V tasks with defined inputs and outputs, and establishment of documentation conventions provide measures to ensure that software maintenance activities for the PDS of the HFC-6000 platform maintain the acceptable quality demonstrated through the CGD effort. In addition, the existing organization structure and specified assignment of V&V roles provide acceptable independence of the V&V team from the project development team and its design activities. Based on the review of the cited documents, the NRC staff has determined that the procedures for establishing a software V&V plan exhibit the management, implementation, and resource characteristics identified in SRP BTP 7-14 and are, therefore, acceptable for the maintenance of the PDS.

3.2.2.10.2 Verification and Validation Reports

The acceptance criteria for implementation of software V&V activities are contained in SRP BTP 7-14, Section B.3.2.2, "Acceptance Criteria for Software Verification and Validation Activities." This section states that RG 1.168 endorses IEEE Std 1012-1998, and IEEE Std 1028-1997, "IEEE Standard for Software Reviews and Audits," as providing methods acceptable to the NRC staff for meeting the regulatory requirements as they apply to V&V of safety system software.

The acceptance criterion for software V&V implementation identified in SRP BTP 7-14 is that the tasks in the SVVP have been carried out in their entirety. Documentation should exist that shows that the V&V tasks have been successfully accomplished for each life cycle activity group. In particular, the documentation should show that the requirements, design, code, integration, and installation design outputs satisfy the appropriate software development functional and process characteristics.

As described in Section 3.2.1 of this SE, the operating software of the HFC-6000 platform was developed over a long history to support prior product lines of HFC (and the preceding Forney Corporation). Consequently, the PDS was not developed under the HFC software QA program and, instead, was commercially dedicated. Therefore, software V&V reports for the PDS of the HFC-6000 platform are not available. However, review, inspection, and testing activities were conducted as part of the CGD process. These activities were conducted under the HFC QA program and, although they cannot demonstrate the implementation of the full SVVP, the documentation of these activities gives evidence of the implementation of quality processes. In particular, code inspections and validation testing were conducted as part of the dedication effort. The assessment of the evidence from these activities is addressed in Sections 3.2.1.1 of this SE. In addition, the dedication effort involved reconstitution of software design documents with an associated requirements traceability assessment. The RTM is discussed in the next section. The design documents themselves are discussed in Section 3.2.3 of this SE. The documented findings from these activities were also subject to review and audit during the course of this evaluation. In particular, selected code review and test records were inspected as part of the on-site regulatory audits at the HFC facility (References 15 and 16). Based on the review and audit of the available documents identified in the referenced sections of this SE, the NRC staff determined that the execution of the dedication activities was consistent with the applicable HFC procedures and, therefore, provides an adequate means to ensure the quality and functionality of the reconstituted design documents and other outputs of the dedication process.

3.2.2.10.3 Requirements Traceability Matrix

The definition of a RTM is contained in SRP BTP 7-14, Section A.3, "Definitions," states: "An RTM shows every requirement, broken down into sub-requirements as necessary, and what portion of the software requirement, software design description, actual code, and test requirement addresses that system requirement." This is further clarified in Section B.3.3, "Acceptance Criteria for Design Outputs," in the subsection on Process

Characteristics. This section states that a RTM should show what portion of the software requirement, software design description, actual code, and test requirement addresses each system requirement.

The dedication of the PDS of the HFC-6000 platform involved reconstitution of software documentation and the inspection and testing of the software. To facilitate the dedication process and contribute to the demonstration of quality, a RTM was generated to enable requirements for the PDS to be traced through testing. RR901-000-31, "HFC6000 Product Line (Pre-Developed Software – PDS) Traceability Matrix" (Reference 97), documents the RTM for the operating software of the HBC-SBC06 controller card for the SC processor, the SAP processor, and the SEP processor. It also documents the RTM for the VHDL code implemented in the CPLDs that perform management of PCB addressing and control for the HFC-SBC06 and HFC-DPM06 modules. The three attachments (Reference 98, 99, and 100) document the extension of the RTM for the CQ4 requirements, the EI requirements, and the I/O module software requirements. The RTM provides the enumerated PDS requirements cross-referenced against the corresponding design description, source code, source code review record, and test references. The cross referencing identifies what portion of the design description and test documents address the implementation and testing of a specific requirement.

Two regulatory audits were conducted (References 15 and 16) in which the RTM was used to assist in demonstrating the completeness of the requirements, confirm forward and backward traceability, and assess the coverage of the requirements by the validation testing. Some issues were identified in the audits and subsequently addressed by HFC (References 70, 78, 101, and 102). The corrective actions involved revision of the requirements specification and RTM and development and execution of a revised test case. Subsequent review of the revised documents and the corrective action records, submitted as part of the initial and revised response by HFC to RAI Part 3 (References 17 and 18), confirm that the anomalies have been resolved.

Based on the review of the RTM, the results of the audits, the corrective action records, and the HFC response to RAI Part 3, the NRC staff reached several determinations about the requirements and the RTM. The requirements are found to be clearly identified and broken down to an appropriate level in the RTM. The RTM adequately cross-references each requirement with the appropriate portions of the design descriptions, source code, source code review records, and tests. Consequently, the requirements are found to be traceable, complete, consistent, and verifiable. The NRC staff concludes that the requirements tracing process, as implemented in the RTM, provides reasonable assurance that all of the operating system requirements are correctly implemented in the PDS of the HFC-6000 platform and is, therefore, acceptable. The traceability analysis findings for the HFC-6000 operating software, as documented in the cited versions of RR901-000-31 and its associated attachments, are suitable as input for project-specific analyses to support safety-related usage of the HFC-6000 platform. However, additional tracing analyses for specific safety-related projects must address traceability to the application requirements and the dependence of the application software on operating system functionality.

3.2.2.11 Software Configuration Management Plan

The acceptance criteria for software configuration management plans (SCMPs) are contained in SRP BTP 7-14, Section B.3.1.11, "Software Configuration Management Plan (SCMP)," and Section B.3.2.3, "Acceptance Criteria for Software Configuration Management Activities." These sections state that both: (1) RG 1.173 that endorses IEEE Std 1074-1995, Clause A.1.2.4, "Plan Configuration Management," and (2) RG 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," that endorses IEEE Std 828-1990, "IEEE Standard for Configuration Management Plans," provide an acceptable approach for planning configuration management. SRP BTP 7-14, Section B.3.1.11 further states that additional guidance can be found in IEEE Std 7-4.3.2-2003, Clause 5.3.5, "Software configuration management," and in Clause 5.4.2.1.3, "Establish configuration management controls." NUREG/CR-6101, Section 3.1.3, "Software Configuration Management Plan," and Section 4.1.3, "Software Configuration Management Plan," also contain guidance.

Configuration management provides the methods and tools to identify and control the system and programming throughout its development and use. Activities include: (1) the identification and establishment of baselines, (2) the review, approval, and control of changes, (3) the tracking and reporting of such changes, (4) the audits and reviews of the evolving products, and (5) the control of interface documentation. Configuration management is the means through which the integrity and traceability of the system are recorded, communicated, and controlled during both development and maintenance. The Software Configuration Management Plan (SCMP) needs to include an overview description of the development project and identify the configuration items that are governed by the plan. The plan should also identify the organizations, both technical and managerial, that are responsible for implementing configuration management.

Software configuration management for the HFC-6000 platform is established by WI-ENG-003. This WI provides the software configuration management (SCM) strategy for HFC and serves as the basic SCMP. The HFC SCMP defines the SCM roles and responsibilities for internal organizations and staff, identifies the SCM tools, and describes the processes for SCM including SCM item identification, configuration control activities, change control authority and request mechanisms, and change/error tracking and reporting (in conjunction with the CAP as discussed is Section 3.2.2.6 of this SE). The Director of Engineering has overall responsibility for product line and project SCM items. The Engineering Department designates a SCM owner of each software development item and, according to WI-ENG-020 (Reference 83), also provides a software engineering manager to be responsible for the items in the software repository. The V&V team is designated as SCM owner of each V&V item and also has the responsibility to audit the SCM process and records at the end of each life cycle phase for a project. As specified in QPP 1.2, the QA Department provides a document control coordinator to be responsible for the document library.

Software requirements, software and hardware design documents, software source codes for both application and operating software, V & V plans and products, and test procedures and records are among the items identified in WI-ENG-003 for configuration control. The V&V implementing instruction, WI-ENG-022, also specifies that configuration of the tools used in the software development process will be maintained under the SCM program. Each SCM item is given a unique identification for control and tracking by product name or document number, version, and baseline component identification (e.g., part number) and date. The baseline identification (ID) number indicates the generation of the item and is related to a revision/change history in the SCM database. The HFC SCMP uses a project life cycle model to control each identified item and define the change process. An item may go through many intermediate baselines before reaching its final baseline milestone at product release.

Documents are maintained in physical and electronic form. Record hard copies are maintained in an access controlled reference library and electronic files are stored on a server, with tracking and records provided by the Serena Software PVCS Version Manager software. Source code, object files, executable code, and project-specific build files are archived in a repository using Microsoft Visual SourceSafe; however, version control for the IOM operating software is provided by PVCS Version Manager. A part number is assigned to uniquely identify the source code. Since object files and executable code can be regenerated from the identified source codes, it is the source code itself that is under version control and change control mechanisms. Changes to build files are tracked by project.

After operating software has been released to form a final baseline for the firmware associated with each of the three processors on the HFC-6000 controller module or the processor for an I/O module, the binary executable code is burned onto PROMs using a dedicated fixture. The resulting PROMs are then installed in the PCB for the appropriate HFC-6000 module. Software identification for firmware consists of a header that identifies the operating software type (i.e., SC, SAP, SEP) and the build date for the specific implementation. An internal checksum is also provided in the first byte of the code. In addition, a part number label is applied to each PROM. However, the software part number is not embedded in the firmware.

The Bill of Materials (BOM) for a project (such as ERD-111 Qualification Project for the HFC-6000 platform) contains identifying information on the hardware and software components of a system. The hardware modules are identified by a module type and part number. The firmware components are identified in the BOM by part number and checksum. In addition, each project generates a master configuration list (MCL). For example, the MCL for the qualification test specimen for the ERD-111 project is recorded in a Microsoft Excel spreadsheet file containing part numbers, revision letters, serial numbers, board types, and software part numbers for the constituent components of the representative system.

Software SCM records are maintained and can be cross-referenced against the BOM and physical ID on the modules for a specific project. Physical ID on the PCB of a module is provided by stickers that are attached during assembly and configuration. A bar code sticker on a card contains the serial number for the specific item, the part number for the module, and the build (i.e., manufacture) date. An additional sticker identifies the module revision by noting the letter assigned to that particular revision. Stickers on the onboard CPLDs and PROMs provide software part numbers for CPLD logic and processor firmware, respectively. The firmware is not modifiable in the field. Operating software identification (i.e., the checksum and header of the firmware) can only be checked using the HFC development and maintenance tools while the module is out of service (i.e., not installed in the safety cabinet). Direct queries are not supported while a controller is in normal operation mode based on configuration settings (i.e., onboard switches and jumper settings). Once this identifying information is accessed with the module in an out-of-service development, test, or maintenance environment, cross checks of the build date and checksum with the correlated part numbers in the BOM and the stickers on the card are a means for confirming that the correct software is installed.

Section 10.1.3.3 of the TR notes that subcontracted vendors may manufacture PCBs for the HFC-6000 platform, and those vendors would be provided the approved operating software and training for installation and testing of the resulting firmware. In the absence of confirmation that the vendors are Appendix B suppliers, the potential exists for version errors in the installation. During the second regulatory audit at the HFC facility (Reference 16), the audit team was able to inspect a firmware checkout procedure and final acceptance report for a recently completed project. The inspection and test documentation contained a printout of all the checksum data and software build dates for each component. Any discrepancies in software version clearly would have been identified for correction prior to shipment. Although the checkout procedure was executed as part of the quality plan developed specifically for that project, it is not explicitly specified in the governing procedures for establishing SQAPs that were evaluated in Section 3.2.2.3 of this SE. Therefore, it is an ASAI to confirm that all firmware versions are directly validated at the HFC testing facility prior to shipment. The measures to assure the appropriate configuration management of the installed operating software will be evaluated as part of a plant-specific review.

Under the HFC SCMP, the change control process is managed to ensure that unauthorized access and software changes of inadequate quality are prevented. Similarly to the CAP described in Section 3.2.2.6 of this SE, the SCM change control process uses the Serena Software PVCS Tracker software to manage and track change requests. The tool automatically routes an SCR to enable impact analysis, implementation approval and implementation signoff to be executed and tracked. During a development project, the owner of a SCM item has responsibility for review and approval. The change request can be elevated to HFC management if the impact is determined to affect multiple organizations or products. After a SCM item has been released for production (i.e., achieved the final baseline milestone through the HFC software QA program), approval and signoff authority is attributed to HFC management. The change process was described in Section 3.2.2.6 of this SE in terms of the CAP. Key elements include the involvement of the Director of Engineering, V&V team, and QA manager in the approval and sign off process and the access control to the software librarian to ensure version control.

Once the change implementation has been approved, the software engineer designated to implement the modification will use Microsoft Visual SourceSafe to access and track the code versions for software development. The SourceSafe tool serves as a software librarian. It has the capability to enforce varying access permissions for different users. The software engineering manager has authority to grant access rights to users. For IOM operating software, the Director of Engineering has authority to grant access to the PVCS Version Manager tool. [Access levels are set in the software librarian tool.] Access to the source code repository is through networked engineering workstations. The software librarian tool requires an authorized user to check out and reserve the source code before a change can be made. This reservation process uses a “check out” with a lock option so only one user can "check out" a source module at a time. The repository has all archived versions of each operating software component available for reference, as well as records of changes made to each software component. A working copy of the operating software directly related to the change is collected in a local folder for development or maintenance to support a project. The folder is identified by a project designation and the part numbers for the affected software are incremented. The record version of the software remains unchanged in the repository while the development or maintenance activity proceeds.

When the change is implemented, the modified software must go through the formal review and signoff processes before achieving its SCM milestone or being released for production. Thus, the necessary life cycle reviews, analyses, and tests must be completed for the software change to attain signoff by the SCM software item owner, Director of Engineering, V&V team, and QA manager. Following signoff, the SCR can be closed and the software can be prepared for inclusion in the repository as a new software version with its unique part number. While, the modified source code is now a baseline version, it is also required to follow a "check in" process to be placed in the repository. The PVCS Tracker tool records change activities. The available reports include latest version of a baseline component, review and approval status, error report and correction status, open SCRs, impact reports, and product versions that are released for use.

Maintenance of commercially dedicated operating software adheres to the HFC software QA program and follows the configuration management procedures. The CAP provides internal mechanisms to identify errors and initiate corrective action using the SCM process. An SCR provides a means to request, implement, and document approved changes, such as software modification to implement corrective maintenance. Each software revision change is associated with a SCR number. The change history of a software component is maintained in the SCM database by the PVCS Tracker. For a project, the BOM incorporates progression through revisions by identifying the applicable SCRs documenting the software change history.

The configuration management process defined by WI-ENG-003, as augmented by WI-ENG-020 and WI-ENG-022, provides measures to establish version control for the PDS of the HFC-6000 platform. In addition, the SCMP and CAP (i.e., QPP 16.1) provide the process and procedures to ensure that software maintenance activities for the PDS preserve the acceptable quality demonstrated through the CGD program. Specifically, the SCM process for change control contributes to fault correction by providing an authorization structure and resolution tracking mechanisms. As noted above and in Section 3.2.2.6 of this SE, the configuration control mechanisms for software items provide adequate controls to establish a baseline version for software that has undergone change as part of maintenance. Based on a review of the cited procedures, the NRC staff has determined that the SCM process exhibits the management, implementation, and resource characteristics identified in SRP BTP 7-14 and is, therefore, acceptable for maintenance of the PDS.

3.2.2.12 Software Test Plan

The acceptance criterion for software test plans (STPs) is contained in SRP BTP 7-14, Section B.3.1.12, "Software Test Plan (STP)," and in Section B.3.2.4, "Acceptance

Criteria for Testing Activities." These sections state that both (1) RG 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," that endorses IEEE Std 829-1983, "IEEE Standard for Software Test Documentation," and (2) RG 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," that endorses IEEE Std 1008-1987, "IEEE Standard for Software Unit Testing," identify acceptable methods to satisfy software testing requirements.

The purpose for the STP is to prescribe the scope, approach, resources, and schedule of the testing activities and to identify the items being tested, the features to be tested, the testing tasks to be performed, the personnel responsible for each task, and the risks associated with the plan. The test plan should cover all testing performed to the system and programming, including unit testing, integration testing, factory acceptance testing, site acceptance testing, and installation testing. The test plan needs to be understandable, ensure that testing responsibilities have been given to the appropriate personnel, and that adequate provisions are made for retest in the event of failure of the original test.

Testing for HFC products and projects are governed by the procedure for design control, QPP 3.1 and the procedure for the software lifecycle and V&V program, QPP 3.2. The V&V team leader is responsible for the generation and/or evaluation of test plans while the design engineers are responsible for generation of test plans/procedures/cases and the execution of tests. Design validation tests are specified in the procedures. These tests include individual component testing, prototype testing of modules, qualification testing of applications, and acceptance testing of systems. In particular, the QPP 3.1 specifies comprehensive design verification testing of firmware (i.e., the operating software) in accordance with the WI for software V&V, WI-ENG-022, which identifies structural testing as necessary. Where modifications for error correction are accomplished as part of the maintenance and corrective action processes, regression testing is specified to validate the modified software. Comprehensive functional testing of the integrated software is specified for applications.

WI-ENG-022 establishes the specific validation requirements for the software V&V program by defining when, how, and by whom specific V&V activities are to be performed. Specifically, the WI identifies the role of the V&V team for testing as performing or overseeing software validation testing. Preparation of test plans, procedures and reports may be performed either by the V&V team or the project development team. In the later case, the V&V team oversees the conduct of these validation activities by reviewing documentation and witnessing tests. For example, the V&V team reviews software-testing records to ensure that structural testing has been performed to validate all branches of a software unit or module. The V&V team also confirms that the test procedures for system validation are developed in accordance with the SSP, address the requirements of the design, and encompass the full range of usage for the system. Software documentation produced in the execution of the QA program includes test plans, cases, procedures and reports. Traceability of all tests performed on software elements is maintained under configuration management control.

As was the case for the SDP and SMP, the STP for software implemented on the HFC-6000 platform is incorporated into a project-specific development plan. As previously noted, development of application software for a plant-specific implementation is outside the scope of the review. Also, the commercially dedicated operating software of the HFC-6000 platform was developed prior to the establishment of the HFC QA program. Consequently, a specific STP addressing the PDS or its maintenance is not available. However, the CGD activities for the PDS addressed a range of validation testing. The effort to dedicate the operating software and generically qualify the HFC-6000 platform for safety-related usage included software object testing, software component testing, and prototype and functional testing. The evaluation of the software testing conducted for the HFC-6000 platform is documented in Sections 3.2.1.1.2, 3.2.1.1.3, and 3.2.1.1.4 of this SE. The NRC staff observed that the range of testing identified in the procedures defining the STP for the HFC-6000 platform are satisfied by these tests, including the provision of structural testing as part of the software component testing for the operating software.

The software V&V report for the ERD111 project, VV0415, provides a further example of the implementation of a testing plan by HFC. [Note: As an outgrowth of previous control system projects for Korean nuclear power plants, HFC established the Control System Qualification Project, ERD111. The purpose of this project was to develop an HFC product line specifically targeted for use in nuclear safety-related applications. The generic qualification and commercial grade dedication activities conducted under the ERD111 project provide the basis for the TR on the HFC-6000 platform.] As described in Section 3.2.2.6, modifications to the hardware and operating software parameters of the controller and analog input modules of the HFC-6000 platform to resolve an issue of inadequate performance for the product line. Adhering to the testing requirements specified in WI-ENG-022, regression testing was successfully performed in each case to verify that the modifications produced the desired result without introducing any negative impact.

The elements of a software test plan to support maintenance of the PDS of the HFC-6000 platform are provided by the procedures for establishing software life cycle plans and for controlling designs. The testing requirements are further amplified in the WI for software V&V. The conduct of testing to support the dedication of the PDS of the HFC-6000 platform also illustrates the provisions for testing under the HFC software QA program. Finally, the implementation of regression testing as part of the corrective action process governing software modifications provides further evidence of the suitability of the test plan procedural basis to support software maintenance. Based on the review of the cited documents and testing, the NRC staff has determined that the procedures for establishing a software test plan exhibit the management, implementation, and resource characteristics identified in SRP BTP 7-14 and are, therefore, acceptable for the maintenance of the PDS.

3.2.3 Design Outputs

SRP BTP 7-14, Section B.2.3, "Software Life Cycle Process Design Outputs," identifies software documents and products subject to review to evaluate whether the software life cycle development process produced acceptable design outputs. The following documents are included in the review guidance:

- Software requirements specification (SRS)
- Hardware and software architecture description (SAD)
- Software design specification (SDS)

- Code listings
- Build documents
- Installation configuration tables
- Operations manuals
- Maintenance manuals
- Training manuals

It is noted in the review guidance that system requirements documents should also be examined to provide context for a review of software design outputs.

Since this SE addresses the suitability of a digital platform for use in unspecified safety-related applications and does not involve a specific system design, many of the documents identified in SRP BTP 7-14 are not relevant for generic review of a platform. Specifically, operations, maintenance, and training manuals primarily relate to the installed system and support the licensee as end product user. Thus, review of these documents is most appropriate in the context of a specific project. In addition, given that the design of a specific application is not within the scope of this review, some design outputs that are more particularly focused on application software as the object of the development process are not available for review. Since the HFC-6000 operating software is compiled from a dedicated, controlled baseline and implemented as embedded firmware burned onto dedicated PROMs that are directly installed onto PCBs, it is clear that the build documents and installation configuration tables for application software, which are not in the scope of the review, would give more conclusive indication of the effectiveness of the HFC life cycle process. Finally, the operating software of the HFC-6000 platform was developed prior to the establishment of the HFC software QA program so some design outputs were reconstituted as part of the commercial dedication effort or were evaluated under that program (e.g., source code). In particular, documents containing the SRS and SDS were submitted for review. Thus, the evaluation of the available design outputs that correspond to the PDS is focused on the reconstituted requirements and design documents from the dedication effort.

As discussed in Section 2.1 of this TR and presented in PP901-000-02, "HFC-6000 Product Line Document Map" (Reference 20), the HFC design documents are distributed throughout the hierarchical product document structure. The progression begins with product line requirements specification, extends to module requirements and design documentation, proceeds with module detailed design descriptions, and concludes with independent component design descriptions (i.e., hardware or software components that can be used in different modules). As an element of the CGD effort for the PDS of the HFC-6000 platform, a software requirements specification was reconstituted. In addition, software design documentation was also developed as additions to the component design description level of the product line document structure.

3.2.3.1 Software Requirements Specification

The acceptance criteria for an SRS are contained in SRP BTP 7-14, Section B.3.3.1, "Requirements Activities – Software Requirements Specification." This section states that RG 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," endorses IEEE Std 830-1993, "IEEE Recommended Practice for Software Requirements Specifications," and that standard describes an acceptable approach for preparing software requirements specifications for safety system software. The section also states that additional guidance can be found in NUREG/CR-6101, Section 3.2.1, "Software Requirements Specification," and Section 4.2.1, "Software Requirements Specification."

Without requirements from a plant-specific system to drive the implementation of a system design and development of application requirements, this review is limited to consideration of the SRS in the context of the product line requirements. The requirements for the HFC-6000 platform are contained in RS901-000-01 (Reference 19). The product line requirements specification documents the concept for the product line and provides an architecture overview, list of constituent modules, and high-level requirements for each module. These requirements, coupled with the module requirements cited in the RTM (References 97 through 100) and the safety (Reference 84) and security (Reference 28) considerations, provide drivers for the software requirements of the HFC-6000 operating software.

The SRS for the PDS of the HFC-6000 platform is primarily contained in RS901-000-37, Revision I, "HFC-6000 Controller and HFC-DPM06 SC, SAP, SEP Firmware, VHDL Program Code Requirements Specification" (Reference 103), and its associated appendices (References 104 and 105). These documents address the software requirements for the SC firmware, SAP firmware, and SEP firmware, which correspond to the SYS processor, ICL processor, and C-Link processor, respectively, of the HFC-SBC06 controller module. The requirements for the VHDL logic code of the onboard CPLDs for the HFC-SBC06 and HFC-DPM06 modules are also provided, along with requirements for the UCP point-to-point protocol. The appendices provide requirements for the EI and the CQ4 analog blocks. The requirements for the IOM software are addressed by documents for common I/O requirements (Reference 95) and IOM requirements for each platform module, which are referenced in RR901-000-31, Appendix C, "I/O Card Requirement Traceability Matrix" (Reference 100).

In Section 10.1.2.1 of the TR, HFC claimed that the SRS conforms to guidance and criteria of RG 1.172 and IEEE Std 830-1993. Furthermore, HFC claims that the requirements are traceable, accurate, complete, consistent, ranked for importance or stability, verifiable, and modifiable. In evaluating the HFC claims, the NRC staff noted that the RG and standard both provide guidance directed toward an SRS for a specific application, which would be driven by plant-specific system requirements. Thus, conformance to the guidance must be considered in context and the degree to which the guidance can be satisfied is limited by the absence of a specific application.

To assess these claims, the NRC staff reviewed the requirements documents (listed above). In addition, the NRC staff also reviewed selected portions of the SRS during thread audits conducted at the HFC facility in October and December, 2009 (References 15 and 16). During this audit, the requirements traceability matrix was used to perform forward and backward traces through the SRS, SDS, source code listings and source code review record, and test procedures and results. During the thread audits, a limited number of anomalies were identified related to completeness, unambiguity, and verifiability. The HFC staff reported these findings via CRs that were subsequently addressed through the CAP. The corrective actions involved revision of the SRS to address perceived ambiguity and ensure completeness of the requirements (References 70, 101, and 102) and to ensure variability through thorough validation test procedures (Reference 78). Subsequent review of the modified SRS and test procedures confirmed adequate resolution of the identified issues.

Following treatment according to the HFC CAP, the NRC staff found that the revised SRS demonstrates the characteristics claimed by HFC. Consequently, the NRC staff concurs that the SRS for the PDS of the HFC-6000 platform conforms with RG 1.172 and IEEE 830-1993 to the extent feasible for a requirements specification addressing platform operating software rather than application software. Based on the review of the SRS contained in the cited documents and the findings of the thread audits, the NRC staff determined that the SRS exhibits the functional and process characteristics identified in SRP BTP 7-14 that are necessary to give adequate evidence of quality software for use in nuclear safety applications.

3.2.3.2 Software Architecture Description

The acceptance criteria for the SAD are contained in SRP BTP 7-14, Section B.3.3.2, "Design Activities – Software Architecture Description (SAD)." This section states that the SAD should describe all of the functional and software development process characteristics listed, and that NUREG/CR-6101, Section 3.3.1, "Hardware and Software Architecture," and Section 4.3.1, "Hardware/Software Architecture Specifications," contain relevant guidance.

When performing this review, the NRC staff should be able to refer to this architecture to understand how the software works, the flow of data, and the deterministic nature of the software. The architecture should be sufficiently detailed to allow the reviewer to understand the operation of the software.

The HFC document structure does not provide a standalone document identified as a SAD. However, the software architecture for the HFC-6000 platform is described in several documents. The module design descriptions for the HFC-SBC06 and HFC-DPM06 and the IOMs contain explicit descriptions of the software architecture for the HFC-6000 modules (References 30 and 33). In addition, the detailed design descriptions for the modules provide additional information about the architectures and data flow (References 31 and 34). DS001-000-01 (Reference 44) describes the architecture of the OS execution environment and DS001-000-06 (Reference 47) provides details about data flow through software components and process control under different modes of operation. The program structure and sequence of operation for the EI, which executes the application program, is given in DS001-000-02 (Reference 45). Additionally, the descriptions of the C-Link and ICL protocols define the mechanisms of communication and the deterministic characteristics (References 21 and 49).

A review of the documents identified above confirmed that the description of the HFC-6000 platform software architecture is sufficiently detailed to allow the NRC staff to understand the operation of the software. Specifically, the software architecture documentation adequately describes how the software works and clearly illustrates the data flow among the processors on the controller module and within the platform. Additionally, the task scheduling process and execution sequence of tasks are explained and key communications characteristics are described. The evaluation of deterministic performance is addressed in Section 3.4.2 of this SE. Based on the findings of this review, the NRC staff determined that the documentation of the software architecture, as contained in the cited documents, exhibits the functional and software development process characteristics listed in BTP 7-14.

3.2.3.3 Software Design Specification

The acceptance criterion for the SDS is contained in SRP BTP 7-14, Section B.3.3.3, "Design Activities – Software Design Specification (SDS)." This section states that the software code accurately reflects the software requirements, and that NUREG/CR-6101, Section 3.3.2, "Software Design Specification," and Section 4.3.2, "Software Design Specifications," contain relevant guidance.

HFC does not provide a single, specific document that serves as the SDS. Instead design descriptions at the module and component level document the software design. Each HFC-6000 module has a module design description. These documents provide the functional, architectural, and design descriptions of the module. The module designs for the HFC-SBC06 and HFC-DPM06 modules are captured in MS901-000-01. Since all the IOMs share the same hardware and software architecture and have many similar functions and designs, only one module design description, MS901-000-02, is provided for all the I/O modules.

Given the complexity of the HFC-6000 modules, module detailed design descriptions are also provided. DS901-000-01 documents the detailed designs for the HFC-SBC06 and HFC-DPM06 modules. The detailed descriptions of implementation of each individual IOM, including descriptions of specific I/O functions, are provided in a module detailed design description for each IOM (References 35 through 42).

HFC provides component design specifications that describe architecture, interfaces and implementation information of independent software components, such as the task scheduler and execution environment, communication protocols, and software libraries. Thus, design descriptions for the software components of the PDS of the HFC-6000 platform were submitted by HFC. These documents include the C-Link protocol, the UCP, the OS, the EI, the CQ4 analog blocks, system software components, the redundancy and failover mechanism, and the ICL protocol (References 21, 22, and 44 through 49).

The NRC staff reviewed the design description documents cited above. In addition, the NRC staff inspected the software documentation during thread audits conducted at the HFC facility in October and December, 2009 (References 15 and 16). During the site visits, the RTM (Reference 97) and its associated appendices (References 98, 99, and 100) were used to perform forward and backward traces through the SRS, SDS, source code listings and source code review record, and test procedures and results. The audits demonstrated that the design description documents accurately reflect the software requirements. In addition, based on the review of the documents, the NRC staff determined that the distributed SDS exhibited the functional and software development process characteristics listed in BTP 7-14 based on the review finding that sufficient information on the platform design existed and the design description was sufficiently understandable.

3.3 Environmental Qualification

Two objectives of environmental qualification testing for a safety system are (1) to demonstrate that the system will not experience failures due to abnormal service conditions of temperature, humidity, electrical power, radiation, electromagnetic interference, radio frequency interference, power surge, or seismic vibration, and (2) to verify those tests meet the plant-specific requirements.

Criteria for environmental qualification of safety-related equipment are provided in 10 CFR Part 50, Appendix A, GDC 2, "Design bases for protection against natural phenomena," and GDC 4, "Environmental and dynamic effects design bases." Additionally, the regulation at 10 CFR 50.55a(h), "Protection and safety systems," incorporates by reference the requirements of IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," which addresses both system-level design issues and quality criteria for qualifying devices. RG 1.209, "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants," endorses and provides guidance for compliance with IEEE Std 323-2003, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," for qualification of safety-related computer-based I&C systems installed in mild environment locations.

To comply with the requirements of GDC 4, 10 CFR 50.49, "Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants," and IEEE Std 603-1991, an applicant must demonstrate through environmental qualification that I&C systems meet design-basis and performance requirements when the equipment is exposed to normal and adverse environments.

EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," which was accepted by NRC SE dated July 30, 1998, presents a specification in the form of a set of requirements to be applied to the generic qualification of PLCs for application and modification to safety-related I&C systems in nuclear power plants. It is intended to provide a qualification envelope corresponding to a mild environment that should meet regulatory acceptance criteria for a wide range of plant-specific safety-related applications. The qualification envelope that is established by compliance with the guidance of EPRI TR-107330 consists of the maximum (i.e., extremes) environmental and service conditions for which qualification was validated and the range of performance characteristics for the PLC platform that were demonstrated under exposure to stress conditions. Any plant-specific application is obligated to verify that the qualification envelope provided by qualification to the guidance of EPRI TR-107330 bounds the requirements of the application.

The qualification program developed for the HFC-6000 platform addressed environmental qualification for a mild, controlled environment. The basis for the testing program was conformance with the guidance contained in EPRI TR-107330. The results of the qualification program establish the qualification envelope of the HFC-6000 platform. The testing program was conducted on a type test specimen composed of HFC-6000 modules that were configured into a representative system to execute a test system application program (TSAP). The testing program was designed to demonstrate the capability of the HFC-6000 test specimen to (1) perform defined design functions within specified tolerances under normal environmental and operating conditions and (2) perform design functions within specified tolerances under stress conditions, as specified in EPRI TR-107330, Section 6, "Qualification Testing and Analysis."

In addition to specifying basic capabilities for a generic PLC platform, EPRI TR-107330, Section 4, "System Requirements," contains platform performance criteria addressing analog I/O accuracy, discrete I/O characteristics, isolation among modules and among signal channels within a module, and surge withstand, as well as response times for the various combinations of I/O modules. These performance characteristics establish an acceptable performance envelope that serves as the basis for acceptance criteria defined for the environmental qualification testing program addressed in the guidance.

The environmental qualification envelope specified in Section 4 of EPRI TR-107330 is given in terms of bounding conditions for environmental withstand, electromagnetic interference and radio-frequency interference (EMI/RFI) withstand, and seismic withstand. The environmental withstand test conditions include:

- A temperature range from 4 to 50 degrees Celsius (°C) [40 to 120 degrees Fahrenheit (°F)] and a humidity range of 10 to 95 percent (non-condensing) relative humidity.
- Radiation exposure of up to 10 gray (Gy) [1000 radiation absorbed dose (rad)] is specified as the bounding condition for that environmental stressor.
- A test profile that provides for operational periods of at least forty-eight hours at high temperature and high humidity conditions, then a ramp down period of at least four hours, followed by at least eight hours at low temperature and low humidity conditions, and ending with a temperature ramp up period of at least four hours to ambient conditions.
- Power source ranges are specified as 90 to 150 VAC, coupled with a frequency range of 57 to 63 Hz as an element of the environmental withstand conditions.
- Electrostatic discharge (ESD) and power surge per the guidance regarding conditions and test methods for EMI/RFI in EPRI TR-102323, "Guidelines for Electromagnetic Interference Testing in Power Plants."
- The seismic withstand conditions are specified as the application of five operating basis earthquakes (OBEs) at a vibration level of 9.75 g, followed by the application of a safe shutdown earthquake (SSE) simultaneously applied in three orthogonal directions. The SSE level is given as 14 times the acceleration due to gravity (g).

The test sequence specified by EPRI TR-107330 involves conducting the environmental withstand testing first, followed by the ESD, EMI/RFI, seismic, and surge withstand testing in any order. Prequalification acceptance testing is specified to address software application object testing, initial calibration, system integration, operability and prudency tests, and burn in for the test specimen. The guidance in Section 5, "Acceptance/Operability Testing," of EPRI TR-107330 specifies that the operability tests should address analog I/O accuracy, response time, operability of discrete inputs and outputs, communications operability, co-processor operability (for those platforms supporting a co-processor), timer function accuracy, detection of failure to complete a scan (i.e., application program loop or cycle time), failover operability for redundant configurations, loss of power and power interruption. Prudency tests are specified to address burst of events (BOE), serial port failure, serial port noise, and fault simulation to demonstrate failure detection in redundant configurations. Operability tests confirm functionality while prudency tests demonstrate performance under simulated in-service stresses.

As part of the qualification test program, EPRI TR-107330 establishes test points for the execution of operability and prudency tests on the type test specimen. The test sets are specified for execution during environment withstand testing as follows: (1) both tests following the minimum exposure period at the high temperature and high humidity conditions, (2) operability test only following the minimum exposure period at the low temperature and low humidity exposure, and (3) operability test only after the test specimen has been returned to stable ambient conditions. During EMI/RFI withstand testing, all of the operability tests except for the accuracy tests and only the BOE test of the prudency tests are specified for execution during each susceptibility test. The operability tests are specified for execution following the ESD test. For seismic withstand testing, the operability and prudency tests are specified for execution during the SSE test. Following the SSE test, the operability test is specified for execution. Since the stated purpose of the operability tests are to ensure that the module types under test are functioning correctly, satisfaction of the performance criteria at the specified testing points is necessary to demonstrate qualification.

Based on the evaluation documented in the following subsections, the NRC staff has determined that acceptable qualification of the HFC-6000 has been demonstrated for radiation, power surge, electrostatic discharge, and seismic withstand capabilities. In addition, the NRC staff concludes that EMC qualification for radiated magnetic field, low frequency conducted interference, and high frequency conducted interference emissions has been demonstrated. Furthermore, the NRC staff finds that the HFC-6000 platform has also been demonstrated to provide acceptable isolation among signal channels and I/O modules within a safety-related system. It is an ASAI to establish that the qualification envelope for the HFC-6000 platform bounds the corresponding plant-specific conditions for these environmental stressors and that the performance characteristics demonstrated for the HFC-6000 platform under the tested service conditions are adequate for the specific application (see Section 5.2 of this SE).

The NRC staff concluded that qualification has not been adequately demonstrated for an environmental stress withstand capability (i.e., qualification for temperature and humidity). Also, the NRC staff finds that EMC qualification has not been adequately established for radiated and conducted susceptibility or for radiated electric field emissions. Demonstration of qualification against environmental stress and EMI/RFI constitutes a generic open item (see Section 5.1 of this SE). HFC has committed to conducting a retest of both environmental stress withstand capability and EMI/RFI immunity of the HFC-6000 platform (Reference 106). Until the qualification retest results or other comparable evidence are submitted for review, full environmental qualification for the HFC-6000 platform remains a generic open item.

3.3.1 Qualification Program for HFC-6000 Platform

TN0401, "Master Test Plan" (Reference 107), established the qualification test program and defined the qualification approach, including configuration of a type test specimen and creation of a synthetic application to exercise the specimen. HFC states in the master test plan that the testing of the HFC-6000 test specimen under the specific stress conditions identified in EPRI TR-107330 will confirm that the HFC-6000 platform is qualified to:

- function during and after exposure to abnormal temperature and humidity,
- function during and after operational basis and safety shutdown seismic events,
- function during and after application of EMI/RFI waveform exposures,
- function during and after application of ESD test discharges,
- function during and after exposure to surge test waveforms,
- function under varying conditions of source power quality, and
- demonstrate specified levels of Class 1E isolation while continuing to function after application of the test voltage levels.

A fully functional representative test specimen, complete with a TSAP, was designed and assembled primarily based on the HFC-6000 platform elements identified in Table 1 of Section 2.1 in this SE. Additional modules and components that are not included in the scope of the HFC-6000 platform under review were incorporated in the test specimen design to serve as a potential qualification vehicle for the complete HFC-6000 product line. The details of the test specimen are provided in DD0401, "HFC-6000 Control System Safety-Related Control System Qualification Test Specimen Design Description" (Reference 108). The overall configuration represents the typical hardware arrangement of a redundant safety controller that is physically located in an equipment room, coupled with a remote I/O chassis that is physically located near the equipment under control. Figure 6, which is adapted from Figure 2-1 of Reference 108, illustrates the overall layout of the test specimen and indicates the boundary between the safety-related and nonsafety-related portions of the representative system. The interior boundary that is indicated in the figure encompasses the portion of the test specimen that principally corresponds to the HFC-6000 platform. The main chassis contained redundant HFC-SBC06 controller modules, the HFC-DPM06 module, and a full complement of IOMs. The expansion chassis were fully populated with IOMs. The qualification system included at least one item of every module type identified in the scope of the HFC-6000 platform, as well as types of other modules that were not included for consideration in the TR.

Communication links were also included in the test specimen. The C-Link network for the qualification system consisted of a single node that enables communication with the personal computer (PC) and tester workstations via a gateway/isolation hub. The physical arrangement of the ICL bus took two forms. To represent implementations with a main chassis and expansion chassis in the same cabinet, the ICL traces of the controller chassis were connected by serial cable with corresponding traces on the expansion chassis. To represent implementations where the main chassis is connected to a remote I/O cabinet, a fiber-optic repeater/terminator pair of HFC-ILR06 modules provided the interconnecting ICL interface.

The HFC-6000 test specimen contained a power supply rack to provide operating power to the three chassis that represent the main portion of the controller hardware while the local expansion chassis used separate modular power supplies.

The TSAP served as a synthetic application that was designed to support qualification testing while providing functionality representative of safety-related applications. The detailed requirements and design description of the TSAP are contained in References 109 and 110, respectively. The TSAP was based on a set of simulated control loops and program code to enable operability and prudency testing. The TSAP provided logic to perform the following functions:

- read inputs associated with the operability and prudency tests,
- drive outputs required by the operability and prudency tests,
- provide logic for timer testing, and
- provide algorithms for the simulated control loops.

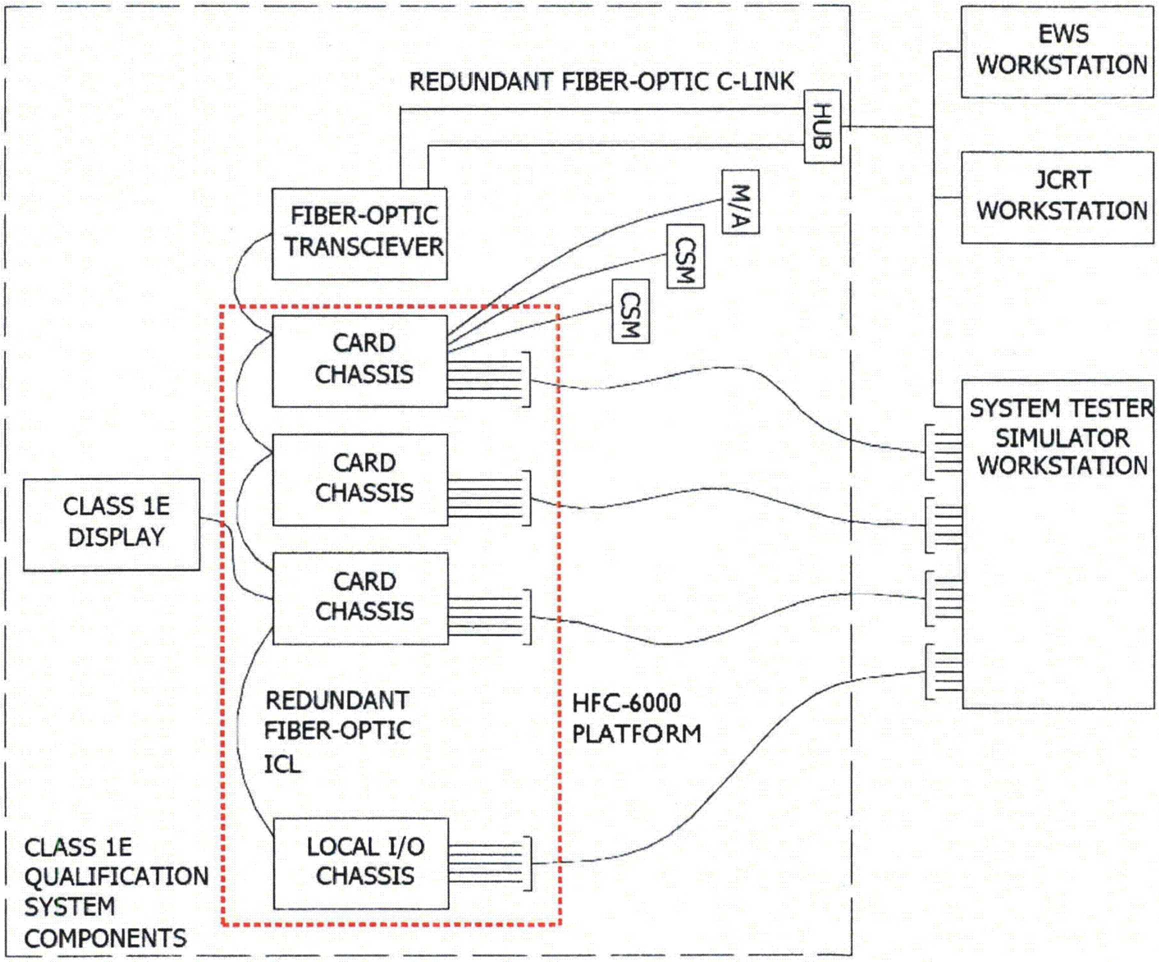

Figure 6 – Arrangement of HFC-6000 Test Specimen [Note: the interior dashed-line box indicates the portion of the test specimen that corresponds to the HFC-6000 platform]

Specifically, the TSAP contained six simulated digital control loops and three simulated analog control loops. These simulated control loops were air circuit breaker control logic, solenoid control logic, non-reversing motor starter control logic, reversing motor starter control logic, simulated ESFAS control logic, simulated main feedwater isolation valve control logic, simulated valve control logic, simulated flow control logic, and simulated level control logic.

In addition to the test specimen, the system tester/simulator was provided to control the functional tests during qualification, stimulate inputs, monitor performance, and capture test results. It consisted of PC workstations, a non-redundant ECS-1200 controller, and an ECS-1200 I/O chassis with the ECS-series card types needed to exercise the I/O channels installed in the test specimen. The PC workstations hosted the automated test software installed along with the complete suite of EWS and Java CRT Workstation (JCRT) software utilities. These utilities provide tools for status monitoring, system control, testing, and maintenance of the overall test system. The ECS-1200 controller had the HFC Plant Automated Tester (HPAT) application program installed to provide specific simulations for the field hardware that the TSAP was programmed to control. This arrangement supported all phases of dynamic testing, including functional verification of system operation and simulation of failure conditions.

The system tester provided both an SOE utility and a Historical Archiving System (HAS) utility to log data generated during the test program. The SOE utility resided on a set of special DI modules configured for a separate controller associated with the HPAT. This utility has a resolution of ±1 ms and was used to record high-speed transitions of digital data points. The HAS utility logged analog and digital data as configured points into a structured query language (SQL) database that resided in the PC workstation of the system tester. Each record in this database included a time stamp as well as point identification.

The following test plans and test procedures were prepared as part of the qualification program for the HFC-6000 platform:

- TN0401, "Master Test Plan" (Reference 108)
- TP0401, "Integration (Setup and Checkout) Procedure" (Reference 111)
- TP0402, "Operability Test Procedure" (Reference 76)
- TP0403, "Prudency Test Procedure" (Reference 77)
- TP0404, "Environmental Stress Test Procedure" (Reference 112)
- TP0405, "Seismic Test Procedure" (Reference 113)
- TP0406, "Surge Withstand Test Procedure" (Reference 114)
- TP0407, "EMI/RFI Test Procedure" (Reference 115)
- TP0408, "TSAP Validation Test Procedure" (Reference 116)
- TP0408B, "Test Specimen Validation Test Procedure" (Reference 117)
- TP0409, "ESD Test Procedure" (Reference 118)
- TP0410, "Burn-in Test Procedure" (Reference 119)
- TP0411, "Isolation Test Procedure" (Reference 120)

The master test plan (Reference 108) provided a link between the testing requirements and acceptance criteria of EPRI TR-107330. The tests were conducted based on the procedures listed above. Individual test plans for each test identify requirements, testing criteria, acceptance criteria, and documentation for a particular test.

To establish the qualification of the HFC-6000 platform, the test specimen was subjected prequalification tests, qualification tests, and post-qualification tests as specified by EPRI TR-107330. The prequalification, post-qualification, and additional in-house testing were conducted at the HFC facility. In addition, isolation testing was performed at the HFC facility.

Following the guidance in EPRI TR-107330, the HFC-6000 qualification test sequence involved temperature and humidity tests, seismic tests, and electromagnetic compatibility tests (including EMI/EFI, ESD, surge withstand, and isolation tests). As part of each qualification test, the test specimen was subjected to the specified environmental extremes to simulate the effect of stress conditions. During each test, the TSAP processed test signal waveforms supplied by the HPAT. To detect any deviation in performance, responses of the test specimen during each qualification test were logged for comparison to the performance baseline established during prequalification testing.

The qualification tests were conducted at Wyle Laboratories in Huntsville, Alabama. The seismic tests were performed after the surge withstand tests. A retest of the seismic tests was also conducted subsequent to the completion of the isolation and post-qualification tests.

In accordance with the guidance in EPRI TR-107330, operability and prudency tests were repeated in whole or in part at various points before, during, and after specified qualification tests to acquire data to demonstrate that the system performance remained within acceptable limits. The test procedures for the operability and prudency tests are given in TP0402 and TP0403, respectively. The operability tests developed for the HFC-6000 qualification program consisted of accuracy tests, response time tests, discrete input operability tests, discrete output operability tests, communication operability tests, timer tests, failover operability tests, loss of power tests, and power interruption tests. Power quality tolerance tests were also provided but were only conducted during the environmental qualification tests. The prudency tests developed for the HFC-6000 qualification program consisted of the BOE test, serial port failure test, and serial port noise test. The test coverage provided by the HFC operability and prudency test sets conforms to the guidance of EPRI TR-107330 with two principal exceptions. First, the test for detection of failure to complete a scan is omitted from the operability tests. Second, the fault simulation test is omitted from the prudency tests.

In assessing the necessity of performing the omitted operability and prudency tests from the test sets specified in EPRI TR-107330, HFC concluded that the failover operability tests addressed the intent of the operability test for detection of failure to complete a scan and the prudency test for fault simulation so these tests were omitted for the test sets. As described in HFC response to RAI Part 3 (References 17 and 18), the rationale for the HFC decision is that each test results in a failover from the primary to secondary controller and the failover operability test achieves the same result. Essentially, the test for detection of failure to complete a scan would force a timeout condition due to a stalled processor or execution failure of the application, and this condition will force failover. Similarly, a detection of a simulated fault would result in the primary controller losing "sanity" and, thus, force a failover. The failover operability test uses power failure and maintenance failover to trigger failovers, but the system response is the same after each failover event.

After reviewing the HFC rationale for the equivalence of the tests, along with the basis for the test of detection of failure to complete a scan as described in EPRI TR-107330, Section 4.2.4.7, "Recovery Capability Requirements," the NRC staff determined that one purpose of the test for detection of failure to complete a scan is to qualify the hardware watchdog timer based on its performance under stress in response to failed condition of the controller. The fault simulation test under prudency testing can provide comparable test coverage. However, the failover operability does not test the hardware watchdog timer. Thus, the NRC staff disagrees with the HFC conclusion and finds that omission of both of these tests from the operability and prudency test sets precludes systematic demonstration of qualification for the hardware watchdog timer.

To address the need for a qualifying test that addresses the watchdog timer, TN901-000-09, "Addendum to TP0402, Revision F" (Reference 79), was submitted by HFC for review. In the revised test procedure, HFC has included a specific test to check the hardware watchdog timer function as part of the operability tests to be conducted during qualification testing. This amended test procedure is adequate to provide evidence of qualification for the hardware watchdog timer if it is executed while the test specimen is exposed to environmental extremes during testing. However, the qualification program conducted for the HFC-6000 platform does not demonstrate qualification of the hardware watchdog timer for the HFC-SBC06 controller module. Qualification of this hardware component is one element of a generic open item regarding demonstration of environmental qualification for the HFC-6000 platform (see Section 5.1 of this SE). Until the qualification retest results or other comparable evidence are submitted for review, full qualification of the hardware watchdog timer for the HFC-SBC06 module remains a generic open item.

3.3.2 Platform Operability Testing (Pre- and Post-Qualification)

As specified in EPRI TR-107330, the prequalification testing consisted of application software object tests (see Section 3.2.1.1.2 of this SE), burn-in tests, initial calibration, system setup and checkout tests, operability tests, and prudency tests. These tests were intended to confirm that the integrated TSAP and HFC-6000 equipment operated as expected and to generate a performance baseline for the test specimen.

The post-qualification tests consisted of operability and prudency tests. These test were performed upon return of the test specimen from Wyle Laboratories following the first seismic tests. The tests were repeated following the isolation tests prior to reshipment to Wyle Laboratories for the seismic retest. These additional baseline tests were designated as "in-house" tests.

The burn-in test was executed for 352 cumulative hours of operation. It established a mature set of modules and spares for subsequent testing by eliminating those modules subject to early-life failures. The system setup and checkout tests consisted of the integration test and the TSAP validation test. The integration test was performed to verify that the hardware, wiring and communication cabling for the test specimen had been properly installed and that communication had been established over each communication link. The TSAP Validation Test Procedure involved source code verification, loop logic testing, and operability and prudency test support verification. In the test summary for these tests (Reference 121), HFC claims that they were successfully executed. However, the data reported indicated that the HFC-AI16F analog input modules were not calibrated as required. Consequently, the test specimen was unable to satisfy the performance criteria for analog input accuracy, as specified in EPRI TR-107330, for most of the subsequent qualification tests. The module was recalibrated prior to the seismic retest and demonstrated the specified accuracy for that stress test. The test procedure for the integration test, TP0401, contains an explicit procedural step instructing that calibration of the input modules be verified. However, this step was not performed. HFC opened a CR to resolve apparent deficiencies in their test procedures, as evidenced by the omitted procedural step. The corrective action involved revision of the procedures to require written affirmation that the calibration is verified (Reference 122). Thus, the deficiency in execution of the system setup and checkout should be resolved for future qualification testing. Nevertheless, the omission of the calibration step results in an inability to demonstrate qualification of the HFC-AI16F module for several subsequent qualification tests in the test sequence. Qualification of this hardware component is another element of the generic open item regarding demonstration of environmental qualification for the HFC-6000 platform (see Section 5.1 of this SE). Until the qualification retest results or other comparable evidence are submitted for review, full qualification of the HFC-AI16F module remains a generic open item.

In addition to the impact of the lack of calibration for the analog input module, the establishment of baseline performance characteristics from the prequalification conduct of the operability and prudency tests was affected by some anomalies involving the capture of test results. Consequently, the prequalification baseline performance envelope for the HFC-6000 test specimen had to be supplemented by test results from post-qualification and in-house testing results. Test summaries and test record details are provided in TS901-000-22, “Baseline Testing Summary Report” (Reference 92), TS901-000-29, “Post Qualification Testing Summary Report” (Reference123), and TS901-000-34, “Seismic Retest In-house Testing Summary Report” (Reference 124).

The anomalous condition for test data capture involved the loss of SOE data for the operability and prudency tests. This data was overwritten during the test period due to a fault in the test data recording process. Although this issue affected the initial baseline tests and several subsequent tests, the problem was detected and corrected prior to the final operability and prudency tests. Subsequent operability and prudency test results were used to supplement the lost data. Thus, the prequalification test data was supplemented with post-qualification test data for the purpose of evaluating the test results and to determine if the acceptance criteria of the qualification tests were met. Based on this composite data, HFC established baseline performance characteristics of the test specimen for comparison with performance before, during, and after test specimen stress tests. The HFC rationale for use of post stress test data to supplement pre-stress test data is based on the contention that the performance of the equipment before the stress tests would have been at least as good as the performance of the equipment after experiencing the environmental stress of the qualification program. The argument was that if the post-qualification performance was acceptable, then the prequalification performance would also be acceptable.

The loss of data was not detected until some qualification tests were conducted. HFC opened a CR to resolve the omission of procedural step during the conduct of the test that contributed to the missing data. The corrective action involved replacement of the test procedures with new procedures that address the identified deficiencies (Reference 125). With the corrective action in effect, future qualification testing should not be subject to data loss of the type experience in the HFC-6000 qualification program.

As stated, post-qualification and seismic retest in-house testing results were used to supplement the prequalification results to establish a baseline performance envelope for the HFC-6000 test specimen. However, this approach did not address lost data from the temperature and humidity tests, which compromise the ability to demonstrate qualification for some modules based on missing evidence regarding performance. Based on the summary results from the environmental stress tests (Reference 126), data loss affected qualification results for digital response time, analog response time, timer function, and digital BOE tests. The impact of this condition on demonstration of qualification under temperature and humidity stress is discussed in the next section.

The test summary for baseline testing reported that the power interruption test was failed by the PSM for the HFC-6000 platform. The power interruption test specified a 40 ms interruption in the primary AC power line to the test specimen. When this disruption was imposed with all spare chassis slots filled with operating modules, the internal power monitors for one or more of the modules initiated a reset. After the AC power source was restored, normal operation resumed. Consequently, the redundant power supplies of the HFC-6000 platform were not able to demonstrate the 40 ms hold up time specified by EPRI TR-107330. The conclusion by HFC from this test was that redundant sources of AC power are necessary to satisfy the power supply hold up time performance capability. Consequently, HFC committed to define an interface requirement that all installations include two independent power sources for the redundant HFC-6000 power supplies. Thus, it is an ASAI to provide two independent AC power sources to separately supply the redundant PSM groups within the HFC-6000 power supply rack to ensure that adequate hold up time is provided for power interruption conditions (see Section 5.2 of this SE).

Based on review of the baseline performance envelope from the test summary reports of the prequalification, post-qualification, and seismic retest in-house testing, it is determined that the test specimen did not establish satisfactory performance for analog response time, timer function, or C-Link communication operability. In response to RAI Part 3 (References 17 and 18), HFC reanalyzed the data from the seismic retest in-house tests. TN901-000-07, "Addendum to TS901-000-34 Rev B, Seismic Retest In-house Testing Summary Report" (Reference 127), documents those findings. The clarified test results confirm that the test specimen satisfies the performance criteria from EPRI TR-107330 for all tested characteristics except response time. The digital response time for baseline testing satisfies the EPRI TR-107330 on average but the analog response time is more than an order of magnitude greater than the 100 ms criterion.

As part of the corrective action for a CR established to resolve discrepancies in test summary results and detailed test report appendices (References 15 and 128), HFC generated two summary documents to clarify the qualification results. In RR901-000-37, "ERD111 Performance Envelope" (Reference 93), HFC compiled the qualification test data to more clearly identify the demonstrated performance envelope of the HFC-6000 test specimen under the ERD111 qualification program. In RR901-000-41, "HFC-6000 Qualification System vs EPRI TR 107330 Operating Envelope" (Reference 129), HFC documented the qualification envelope for the test specimen through direct comparison of the qualification test results against the EPRI TR-107330 criteria. These documents were submitted for review as part of the HFC response to RAI Part 3 (Reference 17). Review of the summary documents for the qualification and performance envelopes indicated some inconsistencies and variations in interpretation still remain in the various compilations of data among the multiple reports. Subsequent analysis by HFC resulted in further clarification of the test results through addenda to the original test summaries and an additional clarification document. These documents were submitted to support the TR evaluation and consist of TN901-000-05, "Addendum to TS901-000-23 Rev C, Environmental Test Summary Report" (Reference 130), TN901-000-06, "Addendum to TS901-000-29 Rev B, Post Qualification Testing Report" (Reference 131), TN901-000-07 (Reference 127), TN901-000-08, "Addendum to TS901-000-35 Rev B, Seismic Retest Summary Report" (Reference 132), and TN901-000-12, "Clarifications to Qualification Test Results" (Reference 133). The summary information in RR901-000-37, coupled with the subsequent addenda and clarification, provides confirmation that credible analog response time performance was demonstrated following hardware and software maintenance of the HFC-AI16F module to address compliance with performance requirements.

The modification of the HFC-AI16F module to satisfy the response time performance criterion did not add or change any functionality of the module but instead corrected unacceptable performance. [

] The modification allowed the module to more closely comply with analog response time requirements for the platform. Following the modifications, the demonstrated analog response time for the test specimen ranged from 200 to 380 ms. Digital response time for ambient conditions had been demonstrated in the range of 30 ms to 180 ms. On the basis of these values, the HFC-6000 platform still does not fully comply with criterion of an 100 ms response time, as specified in Section 4.2.1, "General Functional Requirements," Item A, "Response Time," of EPRI TR-107330. Nevertheless, the HFC-6000 platform has demonstrated a credible baseline capability for response time performance that can reasonably service safety functions (see Section 3.4 of this SE) pending analysis of the specific safety application. However, qualification of analog response time performance has not been demonstrated with the platform subjected to environmental stress conditions. Qualification of this performance characteristic is another element of the generic open item regarding demonstration of environmental qualification for the HFC-6000 platform (see Section 5.1 of this SE). Until the qualification retest results or other comparable evidence are submitted for review, qualification of the analog response time for the HFC-6000 platform to establish a comprehensive, credible qualified performance envelope remains a generic open item.

The synthetic application program used for the qualification program is not intended to be an optimized code nor implement a simple safety function. It is noted that the actual response time for any particular system will depend upon the actual system configuration, and may vary significantly from simple to complex systems. Thus, the determination of the suitability of the HFC-6000 platform response time characteristics for a particular application is a plant-specific requirement and, therefore, is an ASAI that is subject to plant-specific review (see Section 5.2 of this SE). Thus, the capability of the HFC-6000 platform to satisfy application-specific requirements for system response time must be determined on a plant-specific basis in terms of the validated system design in relation to the accident analyses in Chapter 15 of the safety analysis report of the plant. The response time performance baseline is limited to the AI16F analog input module in combination with the DO8J digital output module and the DI16I digital input in combination with the DO8J digital output module. EPRI TR-107330 identifies performance criteria for a more expansive range of input-output module combinations. It is an ASAI to demonstrate acceptable response time for other input-output combinations as needed (see Section 5.2 of this SE).

3.3.3 Environmental Stress (Temperature And Humidity) Testing

Clause 3.14, "Mild Environment," of IEEE Std 323-2003 defines a mild environment as an "environment that would at no time be significantly more severe than the environment that would occur during normal plant operation, including anticipated operational occurrences." The environmental conditions under which the HFC-6000 is required to operate are given in Section 4.3.6, "Environmental Requirements," of EPRI TR-107330. In addition to the specifying that the test specimen continue functional operation throughout the test period, acceptance criteria requires that detailed performance characteristics recorded during and after the environmental stress test must remain within acceptable tolerances compared with the performance baseline profile obtained during prequalification testing.

The environmental stress test exposed the test specimen to extremes of temperature and humidity. This testing was accomplished by enclosing the test specimen in an environmental test chamber at Wyle Laboratories. The test specimen was running the TSAP throughout the test period, and its operation was monitored by SOE and HAS data loggers located outside the test chamber. In addition, comprehensive functional tests (i.e., operability and prudency tests) were conducted before, during (at specified points), and after the stress testing. The results of these tests were used to identify any deterioration in functional performance of the test specimen due to adverse environmental conditions. TS901-000-23, "Environmental Testing Summary Report" (Reference 126) documents the test summary and detailed test record. TN901-000-05 (Reference 130) and TN901-000-12 (Reference 133) provide updates and corrections to the test summary based on further analysis of the temperature and humidity test results.

The environmental stress test consisted of four major phases:

- A minimum 48-hour period with the ambient temperature at 60 + 2.8 °C [140 + 5 °F] and a relative humidity (RH) of 90% ± 5% (non-condensing).
- A transition period of 4 hours during which the ambient temperature and relative humidity were reduced.
- A minimum 8-hour period with the ambient temperature at 4 ± 2.8 °C [40 ± 5 °F] coupled with 5% ± 5% RH (non-condensing).
- A transition period of 4 hours during which the test chamber was returned to ambient room temperature and humidity.

Automated subsets of the operability and prudency tests were executed prior to environmental stress testing, at selected points during the period of environmental stress, and after the environmental stress testing. The stress conditions and test points are shown in Figure 7, which was extracted from Figure 9-3 of the TR.

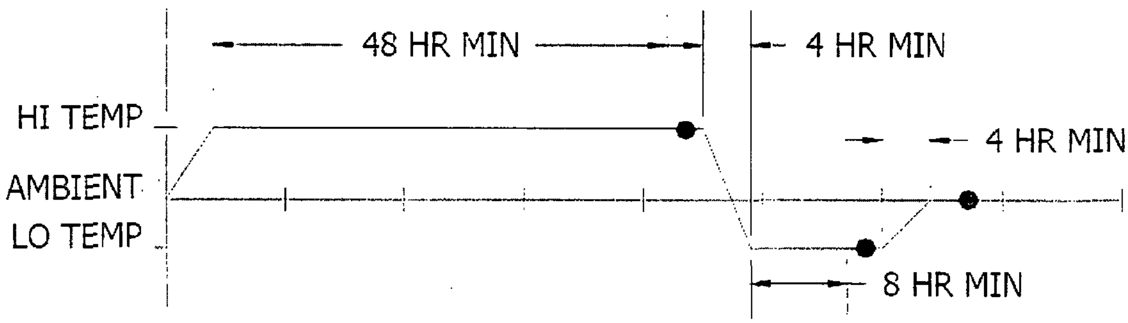

Figure 7 – Environmental stress profile with test points

Some anomalies were observed during the execution of the environmental stress tests. First, the power drop provided by Wyle Laboratories experienced several intermittent failures during the ramp down phase of the temperature tests that resulted in loss of supply power to the test specimen. The cause of the power trips was identified prior to the start of the low temperature period, and it was resolved by obtaining an additional power drop to eliminate the Wyle overload condition. Once power was restored, the test specimen returned to normal operation. All trips of the test specimen were directly correlated to overload of the power drop from Wyle.

[

]

In Section 9.3.3.1 of the TR, HFC claimed that the overall HFC-6000 platform met all acceptance criteria except for verification of the accuracy of RTD input (HFC-AI8M) and AI (HFC-AI16F) modules under environmental stress conditions. Thus, HFC acknowledged that additional project-specific testing may be needed for applications requiring specific documentation of either of these performance characteristics. However, the NRC staff review of the test summaries, addenda and corrections, and detailed records determined that qualification was not demonstrated for the following performance characteristics:

- I/O accuracy (HFC-AI16F, HFC-AI8M, and HFC-AI4K modules)
- Analog response time
- Digital response time
- Communication operability (C-Link, ICL)
- Power interruption tolerance (power hold up capability)
- Power quality tolerance

These findings are based on the absence of test results because either the performance characteristics were not directly measured (e.g., digital response time – only program loop cycle time reported since digital trip output signal was not recorded) or not available (e.g., analog response time, AI accuracy), the test was not completed or data was not reported for specified stress conditions (e.g., power quality tolerance, power interruption tolerance, ICL operability, C-Link operability at high temperature/humidity conditions), or the results did not satisfy the acceptance criteria (e.g., AI accuracy). In addition, it was noted in Section 3.3.1 of this SE that the test addressing the hardware watchdog timer was not performed so qualification of the watchdog timer for environmental stress withstand was not demonstrated.

Based on the review of the HFC documentation of the temperature and humidity test results, the NRC staff determined that qualification of the HFC-6000 platform for environmental stress withstand was not acceptably demonstrated for several key performance characteristics that are necessary to establish suitability for use in safety-related applications. Therefore, the qualification of the HFC-6000 platform under temperature and humidity stress conditions remains as a principal element of the generic open item regarding demonstration of environmental qualification for the HFC-6000 platform (see Section 5.1 of this SE). Until acceptable performance under temperature and humidity stress conditions is demonstrated (e.g., via qualification retest results or other comparable evidence) and submitted for review, qualification of the HFC-6000 platform for environmental stress withstand remains a generic open item.

3.3.4 Radiation Withstand Testing

The guidance on radiation withstand capability that the HFC-6000 platform is required to demonstrate is given in EPRI TR-107330, Section 4.3.6, “Environmental Requirements.” Section 4.3.6.3, “Environmental Withstand Specific Requirements,” of the EPRI guide states that “Evaluations, which provide confidence that none of the components in the PLC platform are degraded by exposure to the radiation level given in the previous section, are adequate for establishing radiation withstand capability.”

Digital systems susceptibility to radiation is discussed in RG 1.209. This RG states that the radiation withstand threshold is different for different types of digital technology, ranging from complementary metal oxide semiconductor (CMOS), which can be susceptible given exposure as low as 10 Gy (1 krad), to bipolar devices, which are not susceptible until exposures on the order of 10 kGy (1 Mrad).

In accordance with the guidance of EPRI TR-107330, HFC performed an analysis of radiation susceptibility for the HFC-6000 platform, which is documented in RR901-000-36, “Radiation Exposure Evaluation” (Reference 134). The HFC evaluation procedure involved the use of publicly available literature and resources to identify the effects of radiation and the radiation exposure limits for each of the semiconductor-based components used in the HFC-6000 platform. The radiation exposure thresholds for the components in the HFC-6000 platform range from a minimum of 25 Gy (2.5 krad) to 3 kGy (300 krad).

Since the most susceptible component for the platform can withstand 2.5 times the 10 Gy (1 krad) withstand level specified in the EPRI TR-107330, the conclusion by HFC is that the HFC-6000 platform as a whole can withstand radiation exposures beyond the EPRI criterion. Based on a review of the HFC method for evaluating susceptibility, the credibility of the data sources, and the technical basis for treatment of radiation exposure as discussed in RG 1.209, the NRC staff finds the HFC analysis of radiation withstand capability to be acceptable and concludes that HFC-6000 platform is qualified to the radiation exposure levels specified in Section 4.3.6.2, "Abnormal Environmental Basic Requirements," of EPRI TR-107330. However, it is an ASAI to confirm that the radiation withstand capability of the HFC-6000 platform envelopes the expected radiation exposure at the point of installation for a system based on the platform equipment (see Section 5.2 of this SE).

3.3.5 Electromagnetic Compatibility Testing (EMI/RFI, ESD, SWC)

EPRI TR-107330 includes electromagnetic compatibility (EMC) testing as part of the overall program to generically qualify a PLC for safety-related application in a nuclear power plant. Specifically, criteria for electromagnetic emissions, electromagnetic interference susceptibility, electrostatic discharge withstand, power surge withstand, and isolation capability are given in Sections 4.3, "Hardware Requirements," and 4.6, "Electrical," of the guide while the qualification approach is specified in Section 6.3, "Qualification Tests and Analysis Requirements." The methods for implementing EMC testing are provided by other referenced guides, as discussed below.

RG 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," endorses Military Standard (MIL-STD) 461E, "Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment," and IEC 61000 series standards for the evaluation of the impact of electromagnetic interference (EMI), radio-frequency interference (RFI) and power surges on safety-related I&C systems and to characterize the electromagnetic (EM) emissions from the I&C systems.

EPRI TR-102323, "Guideline for Electromagnetic Interference Testing in Power Plants," provides alternatives to performing site-specific EMI/RFI surveys to qualify digital safety I&C equipment for a plant's EM environment. In an SE issued in 1996, the NRC staff concluded that the recommendations and guidelines in EPRI TR-102323 provide an adequate method for qualifying digital I&C equipment for a nuclear power plant's EM environment without the need for plant-specific EMI/RFI surveys if the plant-specific EM environment is confirmed to be similar to that identified in EPRI TR-102323.

RG 1.180 states, in the discussion section, that both the RG and EPRI TR-102323 present acceptable means for demonstrating EMC, and that the licensee or applicant has the freedom to choose either method or propose an alternative method. It should be noted that for some types of testing, the maximum acceptable limits for emissions or susceptibility are different and, therefore, it is possible that tested equipment may meet the requirements of one test, and not meet the requirements of the equivalent test from the other document. RG 1.180 states that this is acceptable, as long as the requirements of a complete suite of EMI/RFI emissions and susceptibility criteria from an approved testing approach (e.g., either MIL-STD or IEC) are met, with no mixing and matching of the constituent test criteria and methods.

RG 1.180 provides test methods and limits for suites of conducted and radiated susceptibility tests, conducted and radiated emissions tests, and surge withstand tests. The test limits address the expected EM environment at a nuclear power plant considering extensive long-term in-plant measurements. Alternate suites of test methods, with corresponding test limits providing equivalent characterization of EMC, are provided for each EM phenomena (i.e., emission, susceptibility, and surge). The baseline suite of tests for measurement of EM emissions is drawn from MIL-STD 461E. These four tests are Radiated Emissions (RE) 101, RE102, Conducted Emissions (CE) 101, and CE102. Alternate suites of emissions tests, applicable under specified conditions, are based on IEC 61000-6-4, "Electromagnetic Compatibility (EMC) - Part 6: Generic Standards, Section 4: Emission Standard for Industrial Environments" and Federal Communications Commission (FCC) regulations Part 15, Class A (i.e., 47 CFR Part 15 "Telecommunications, Radio Frequency Devices" Class A digital devices).

The baseline suites of tests for EMI/RFI susceptibility established in RG 1.180 also are selected from MIL-STD 461E, with the corresponding alternate suites of tests based on test methods and limits chosen from IEC 61000-4, "Electromagnetic Compatibility (EMC) - Part 4: Testing and Measurement Techniques." The baseline suite of tests for radiated EMI/RFI susceptibility consists of Radiated Susceptibility (RS) 101 and RS103. The baseline suite of tests for conducted EMI/RFI susceptibility along power leads consists of Conducted Susceptibility (CS) 101, and CS114. Similarly, a baseline suite of tests for conducted EMI/RFI susceptibility along signal leads consist of CS114, CS115, and CS116.

The RG also specifies radiated EMI/RFI testing for frequencies above 1 GHz. The test methods and limits address both emissions and susceptibility and are based on RE102 and RS103.

The baseline suite of tests for power surge withstand testing are selected from IEEE Std C62.41-1991, "IEEE Recommended Practice on Surge Voltages in Low-Voltage AC Power Circuits," and IEEE Std C62.45-1992, "IEEE Guide on Surge Testing for Equipment Connected to Low-Voltage AC Power Circuits." IEEE Std C62.41 defines a set of surge test waveforms while IEEE Std C62.45 describes the associated test methods. Three waveforms are specified: ring wave, combination wave, and electrically fast transients (EFT). Corresponding IEC 61000-4 tests form the alternate suite of tests.

EPRI TR-102323, Revision 1 establishes a testing program based on MIL-Std 461D, "Electromagnetic Emission and Susceptibility Requirements for the Control of Electromagnetic Interference," test criteria and MIL-Std 462, "Measurement of Electromagnetic Interference Characteristics," test methods. For EMI/EFI susceptibility and surge testing, the RS103, CS101, CS114, CS115, and CS116 tests are identified along with corresponding limits. Measurement of emissions involves use of the CE101, CE102, RE101, and RE102 tests, with limits derived from in-plant measurements.

Alternate test methods are identified based on the multipart standards in the series IEC 801, "Electromagnetic Compatibility for Industrial Process Measurement and Control Equipment," which was the predecessor to IEC 61000. In addition, the IEEE Std C62.45 tests are identified as alternate methods for surge testing. The specified surge waveforms are the combination wave and EFT. An optional test is also specified to address ESD. IEC 801-2, "Electrostatic discharge requirements," is identified as the test method. The SE approving EPRI TR-102323 as an acceptable method for ensuring EMC, the NRC staff disagreed with the guide regarding the omission of the RS101 test for evaluating susceptibility to magnetic fields. This test was incorporated in the EMC program defined in EPRI TR-102323, Revision 2.

EMC testing for the HFC-6000 test specimen was conducted primarily at the facilities of Wyle Laboratories. The test results are described in TS901-000-25, "EMI/RFI, ESD, and SWC Testing Summary Report" (Reference 135) and TS901-000-28, "Isolation Testing Summary Report" (Reference 136). The EMC test program involved EMI/RFI testing, ESD testing, surge testing, and isolation testing. During EMC testing, the HFC-6000 test specimen was mounted in open instrument racks. No additional cabinet or cable shielding was installed, and no additional noise filters or suppression devices were used on the input/output interfaces. Therefore, the test specimen was fully exposed to radiation from an external source or open to emit radiation generated internally.

To begin the testing program, the test specimen was subjected to EMI/RFI testing to determine its susceptibility to EMI/RFI noise and the magnitude of EM noise it generates during operation. This test sequence covered a series of four separate testing phases. During the first two test phases, the test specimen was exposed to an external source of EMI/RFI, and the functional operation of the equipment was monitored for signs of degraded operation. During the remaining two test phases, the test specimen was configured for normal operation, and the magnitude of EM radiation generated by the equipment was measured. The sequence of EMI/RFI tests involved testing based on RS103 for the first phase, CS101 and CS114 for the second phase, RE101 and RE102 in the third phase, and CE101 and CE102 in the fourth phase.

Following EMI/RFI testing, the HFC-6000 test specimen was then subjected to simulated ESD pulses to establish its capability to withstand such discharges without disabling or disrupting normal operation. ESD testing was based on the test methods for applying the ESD pulses as defined by IEC Std 61000-4-2.

The HFC-6000 test specimen was subsequently subjected to surge withstand testing through the injection of a large amplitude surge waveform at specified points. The purpose of this test was to demonstrate that Test Specimen performance characteristics remained within acceptable limits during and after exposure to such discharges. The test specimen was powered on and running the TSAP when the test pulses were being applied to specific circuits. Surge withstand testing was conducted using both combination and ring waveforms.

Following the return of the test Specimen from Wyle Laboratories to the HFC facility, isolation testing was conducted to demonstrate that the test specimen satisfies Class 1E isolation requirement among channels within an I/O module (i.e., I/O ports) and among I/O modules within the same system. The tests addressed channel-to-channel and module-to-module isolation for each of the individual I/O module types. The primary purpose of these tests was to demonstrate immunity to faults from the inputs to the I/O modules, not to qualify the modules as Class 1E isolation devices. The test signals were applied to I/O channels both in the main chassis of test specimen and to remote I/O channels in the expansion rack.

3.3.5.1 EMC Emissions Testing

The objective of EMC emissions testing is to ensure that the new equipment will not interfere with the function or operation of existing power plant equipment. The guidance on emissions testing that the HFC-6000 platform is required to satisfy is given in Section 4.3.7, "EMI/RFI Withstand Requirements," of EPRI TR-107330, with reference to Section 7, "Plant and Equipment Emissions Limits," of EPRI TR-102323, Revision 1. EPRI TR-102323 identifies four MIL-STD tests to determine equipment emissions: RE101, RE102, CE101, and CE102.

Radiated emissions tests for specified locations in proximity to the test specimen were performed for magnetic field emissions between 30 Hz and 100 kHz based on the RE101 measurement method and for electric field emissions between 10 kHz and 1 GHz based on the RE102 measurement method. For the RE101 test, measurements were performed with a loop antenna placed at different locations around the test specimen at a distance of 7 cm away. Separate RE102 tests were performed from locations at the front center and rear center positions in relation to the test specimen using horizontal and vertical antennas at a distance of 1 meter away. Conducted emissions tests for specified signal and power leads were performed between 30 Hz and 50 kHz based on the CE101 measurement method and between 50 kHz and 400 MHz based on the CE102 measurement method. Specified portions of the operability and prudency tests were executed during the emissions tests to ensure that the controller was actively operating while the measurements were being conducted. The detailed test results are described in TS901-000-25 (Reference 135).

Although the tests were conducted following the guidance of EPRI TR-102323, the analysis of the test results was based on the test limits from RG 1.180. The NRC staff finds this approach to be acceptable because the test methods from the two guides are equivalent (i.e., virtually identical versions of the same tests from different generations of the standard) and the application of RG 1.180 test limits does not violate the prohibition against mixing and matching test methods (e.g., using MIL-STD tests for low frequency conducted emissions and IEC tests for high frequency conducted emissions). Based on comparison of the test results against the limits from RG 1.180, the HFC-6000 platform met the acceptance criteria for the RE101, CE101 and CE102 emissions tests.

The results from the RE102 emissions test showed at most 5 points exceeding the test limit in the RG. The excessive emissions, taken from the rear of the test specimen, ranged from 0.9 decibels (dB) to 2.5 dB above the limit. In Section 9.3.3.2.1 of the TR, HFC noted that the test specimen was tested in an open instrument rack configuration so the shielding normally provided by the cabinet enclosure was not included. In addition, the assessment of the results by HFC attributed two spikes to modules that are not included in the scope of the HFC-6000 platform. Finally, HFC cited emissions test results for similar fielded HFC equipment (specifically, the Plant Control System for Ulchin Units 5 and 6) that passed the RE102 test when tested in cabinets. [However, these test results were not provided for review along with an analysis of the equivalence of the test systems so no credit for this past experience can be given in this SE.] Thus, HFC concluded that the HFC-6000 platform would also pass the RE102 test in its as-installed configuration. Nevertheless, HFC stated that it would qualify the HFC-6000 platform for electric emission in equivalent cabinet structures on a project-by-project basis.

Based on the review of the test results, the NRC staff concurs that the HFC-6000 platform met the EM emissions acceptance criteria of EPRI TR-107330 and RG 1.180 for radiated magnetic field emissions and low frequency and high frequency conducted emissions. The NRC staff also determined that the HFC-6000 platform did not satisfy the acceptance criteria of the two guides for radiated electric field emissions due to excessive radiated emissions in the frequency range from 10 kHz to 1 GHz.

Furthermore, no EM measurements were reported for radiated electric fields above 1 GHz, as specified in RG 1.180. Therefore, the NRC staff finds the demonstrated emissions characteristics of the HFC-6000 platform to be acceptable for radiated magnetic field emissions, low frequency conducted emissions, and high frequency conducted emissions but not acceptable for radiated electric field emissions. The demonstration of EMC qualification in terms of radiated electric field emissions from 10 kHz to 10 GHz, as specified in RG 1.180, is another element of the generic open item regarding demonstration of environmental qualification for the HFC-6000 platform (see Section 5.1 of this SE). Additional evidence from the EMI/RFI retest can be submitted to resolve the issue generically. Alternately, the EMC qualification for radiated electric field emissions can be treated in plant-specific reviews. Until acceptable control of high frequency radiated emissions is demonstrated (i.e., via qualification retest results or other comparable evidence) and submitted for review, EMC qualification of the HFC-6000 platform for radiated electric field emissions remains a generic open item.

3.3.5.2 EMC Susceptibility Testing

The objective of EMC susceptibility testing is to ensure that equipment will function and operate as designed when installed in the industrial EM environment of a power plant. The guidance on susceptibility testing that the HFC-6000 platform is required to satisfy is given in Section 4.3.7 of EPRI TR-107330, with reference to Appendix B, "EMI Susceptibility Guide," of EPRI TR-102323, Revision 1. In addition, EPRI TR-107330 specifies that each susceptibility test must be performed at 25 percent, 50 percent, and 75 percent of the test level in addition to the specified test level.

EPRI TR-107330 identifies the following acceptance for EMI/RFI withstand testing:

- The main processor continues to function,
- I/O data transfer is not be disrupted,
- Discrete I/O does not change state due to noise, and
- Analog I/O levels do not vary more than 3 percent.

In addition, the EPRI guide states that, for PLC platforms that include redundancy, only the selected value from among the redundant signals needs to meet the acceptance criteria.

However, to establish the qualification envelope, EPRI TR-107330 directs that the performance of the PLC platform during EMI/RFI testing to be reported for all of the test levels used, including the performance of each module for each of the test levels. In addition, Table 5.1, "Operability and Prudency Test Points," of EPRI TR-107330 specifies that the all of the operability tests except for the accuracy tests and only the BOE test of the prudency tests are to be executed during the conduct of the EMI/RFI tests. Since the stated purpose of the operability tests is to ensure that the module types under test are functioning correctly, satisfaction of the performance criteria at the specified testing points is necessary to demonstrate qualification. Also, EPRI TR-102323 states that "All critical, essential, and protected equipment functions should be monitored for acceptable operation and performance before, during, and shortly after [EMC] testing." Furthermore, the susceptibility test is "considered a success if the equipment does not exhibit any malfunction, degradation, or deviation in performance or accuracy beyond documented specification tolerances." Thus, to demonstrate EMC qualification through susceptibility testing, evidence must be provided that the performance criteria specified in EPRI TR-107330 is satisfied, with the substitution of relaxed criteria for analog I/O accuracy.

The execution of the EMI/RFI susceptibility tests for the HFC-6000 platform involved conduct of the three tests identified by EPRI TR-107330 testing guidance in accordance with the MIL-STD methods. However, because of time limitations, several susceptibility tests were only executed at the highest test levels, rather than employing the staged procession of levels for a sequence of tests as identified EPRI TR-107330. The consequence of this deviation from the EPRI guidance is that HFC was not able to generate evidence of EMI/RFI withstand capability for those tests in which the platform did fulfill the acceptance criteria when subject to lower levels of interference.

The radiated susceptibility test specified in EPRI TR-102323 covers a frequency range from 10 kHz to 1 GHz. Performance of the test, based on the RS102 test method, was divided into several frequency ranges with a different signal source and antenna for each frequency range. Each test phase was executed twice: once with the antenna positioned at front center of the test specimen and once with the antenna at rear center. The low frequency conducted susceptibility test was performed between 30 Hz and 50 kHz. These test signals were injected directly into power leads of the test specimen based on the CS101 test method. The high frequency conducted susceptibility tests were executed between 50 kHz and 400 MHz. These test signals were inductively coupled into the power leads of the test specimen based on the CS 114 test method. Because of time limitations, conducted susceptibility across signals leads was not tested. Specified portions of the operability and prudency tests were executed during the tests to allow the functional performance to be monitored for interference effects during conduct of the tests. The detailed test results are described in TS901-000-25 (Reference 135).

In Section 9.3.3.2.1 of the TR, HFC claims that the HFC-6000 platform met the EPRI TR-107330 acceptance criteria for the RS103 and CS101 susceptibility tests. The report noted that individual HFC-DC33 modules exhibited susceptibility during each test but those specific modules were found to be defective. Other HFC-DC33 modules showed no susceptibility during either test. For the CS114 susceptibility test, the test summary reports that the HFC-AI8M and HFC-DC33 modules exhibited some degree of susceptibility over a majority of the test range. Review of the more detailed record in the appendices of TS901-000-25 indicates that the C-Link communications exhibited susceptibility to frequencies between 3 MHz and 70 MHz, the HFC-AI16F module exhibited instances of susceptibility, and degradation of ICL communications was observed. An assessment by HFC addressed some of the anomalies, but a root cause was not clearly identified in most cases. Also, many of these results were attributed to injection of the test signal at 71 percent strength. Although no claim is made by HFC in the TR, it is clear that the platform did not satisfy the EPRI TR-107330 acceptance criteria for the CS 114 test.

In reviewing the test results, the NRC staff determined that the performance records reported for the platform in TS901-000-25 primarily correspond to pretest monitoring. As noted above, EPRI TR-107330 requires that the specified operability and prudency tests be executed during the conduct of each test and the HFC test summary indicates that to be the case. Therefore, data should have been preserved and analysis of performance reported to establish conformance with the acceptance criteria for EMC qualification. The acceptance criteria specified by HFC in TP0407, Section 5.0, "Acceptance Criteria" (Reference 115), states that "Objective demonstration of these [acceptance] criteria will be provided by the alarm process function and results of the Operability and Prudency BOE tests that will be running while the test signals are being injected to the test specimen." Specifically, the capability of all the processors on the test specimen to continue to function normally cannot be adequately judged without analysis of the performance of the platform under stress conditions. Since incomplete evidence of acceptable performance for the HFC-6000 platform is presented in the test summary document, the NRC staff concludes that EMC qualification of the HFC-6000 platform for radiated electric field (high frequency) interference and low frequency conducted interference has not been demonstrated, as had been claimed by HFC in the TR. Similar analysis reinforces the finding that EMC qualification of the HFC-6000 platform for high frequency conducted interference has not been demonstrated. The demonstration of EMC qualification in terms of radiated electric field susceptibility, low frequency conducted interference susceptibility, and high frequency conducted interference susceptibility is a principal element of the generic open item regarding demonstration of environmental qualification for the HFC-6000 platform (see Section 5.1 of this SE). Additional evidence from the EMI/RFI retest can be submitted to resolve the issue. Until acceptable immunity to radiated electric field interference, low frequency conducted interference, and high frequency conducted interference is demonstrated (i.e., via qualification retest results or other comparable evidence) and submitted for review, EMC qualification of the HFC-6000 platform for EMI/RFI susceptibility remains a generic open item.

EMC qualification guidance provided by RG 1.180 specifies radiated susceptibility testing above 1 GHz. Although this frequency range is not addressed by the EMI/RFI testing guidance in EPRI TR-107330, Revision 1, review of any plant-specific system will address this issue. In addition, RG 1.180 specifies testing of signal leads at tailored susceptibility limits. However, the EMC testing for the HFC-6000 did not include signal lead conducted interference immunity tests because of time limitations. Thus, radiated susceptibility testing over the frequency range from 1 GHz to 10 GHz and conducted susceptibility testing of signal leads are other elements of the generic open item regarding demonstration of environmental qualification for the HFC-6000 platform (see Section 5.1 of this SE). Additional evidence from the EMI/RFI retest can be submitted to resolve the issue. Until acceptable immunity of signal lines to low frequency conducted interference and high frequency conducted interference and platform immunity to very high frequency radiated electric field interference are demonstrated (i.e., via qualification retest results or other comparable evidence) and submitted for review, EMC qualification of the HFC-6000 platform for EMI/RFI susceptibility remains a generic open item.

Finally, the SE on EPRI TR-102323 specifies that radiated magnetic field interference testing based on the RS101 test method is part of an overall EMC testing program. However, EPRI TR-107330, Revision 1, omits this test and, consequently, the EMC program for the HFC-6000 platform did not include RS101 in the test sequence. Thus, signals leads were not tested in the execution of the conducted susceptibility tests for the HFC-6000 platform. In the HFC response to RAI Part (Reference 17), HFC invokes the exception to RS101 by stating that the HFC 6000 equipment is not intended for installation in close proximity to CRTs, motors or high current carrying cables. Therefore, this exception can be addressed in a plant-specific review. It is an ASAI to confirm that HFC-6000 equipment is not installed in close proximity to CRTs, motors, high-current cabling, or other strong radiated magnetic field emitters (see Section 5.2 of this SE).

3.3.5.3 Surge Withstand Testing

The objective of surge withstand testing is to verify the ability of equipment to withstand high-energy overvoltage conditions on power lines. The guidance on surge withstand testing that the HFC-6000 platform is required to satisfy is given in Section 4.6.2, "Surge Withstand Capability Requirements," of EPRI TR-107330.

As specified in EPRI TR-107330, general acceptance criteria are that the test specimen shall continue operating satisfactorily during and after application of the test input waveforms without damage or upset to other modules or disruption of backplane signals that could interrupt the execution of the Test Specimen's function. For redundant configurations, failure of a redundant component is not be considered a failure of the test specimen if the failure does not disrupt overall operation of the test specimen and the failure does not propagate to other modules.

Surge withstand capability testing was performed for the HFC-6000 platform by applying the specified ±3 kV surge. Of the fourteen test points identified in EPRI TR-107330, seven were applicable to the HFC-6000 test specimen configuration. Both combination and ring waveforms were applied at each test point.

As documented in TS901-000-25 (Reference 135), the test specimen met all acceptance criteria for surge withstand testing. These test results further demonstrate that no other modules were damaged or disrupted for each application of the test waveform. Also, no failure propagated to other modules. Some individual components were damaged or disrupted when they were subject to the test pulses, but the remainder of the test specimen continued operating normally before, during, and after application of the test waveform. In particular, the HFC-AI8M module was permanently damaged as was one power supply module. In addition, the hardware interface for one ICL channel was damaged on multiple modules in one expansion rack and the corresponding hardware interface on one redundant controller.

The damage to the ICL interfaces and power supply were acceptable in the context of the test because these components were redundant. The HFC-AI8M module was one of many in the test specimen so it was treated as redundant for the test analysis. However, HFC has not indicated that a system based on the HFC-6000 platform would employ redundant IOM for duplicate measurements. Thus, the AI8M would not necessarily be redundant in plant-specific installations. Based on review of the test results, the NRC staff concludes that the damage to the IOM and the interface hardware for the single ICL channel was likely the result of an applied surge along an interconnecting signal lead. Comparing the testing approach specified by EPRI TR-107330 against the guidance in RG 1.180, the NRC staff determined that the power surge test method employed by HFC in accordance with the guidance of EPRI TR-107330 is not intended for use with signal leads (RG 1.180 limits use of C62.45 to power lines and specifies MIL-STD or IEC tests for signal leads) and the test level specified is excessive (RG 1.180 provides two test levels at 1 kV and 2 kV corresponding to low or medium exposure conditions, respectively). Thus, the NRC staff finds the evidence to provide reasonable assurance that the reported damage to HFC-6000 platform components does not indicate a vulnerability that requires mitigating action, such as the use of surge suppression devices. Nevertheless, it is an ASAI to confirm that the surge withstand capability demonstrated for the HFC-6000 platform bounds the expected electrical surge environment at the site of installation (see Section 5.2 of this SE). Based on the review of the of the test results and assessment of the testing approach, the NRC staff finds that the HFC-6000 platform meets the requirements for surge withstand capability specified in EPRI TR-107330 and is, therefore, acceptable for safety-related applications at nuclear power plants.

3.3.5.4 Electrostatic Discharge Withstand Testing

The objective of ESD withstand testing is to verify the ability of the equipment to withstand the effect of electrostatic discharge. The guidance for ESD testing that the HFC-6000 platform is required to satisfy is given in Section 4.3.8, "Electrostatic Discharge (ESD) Withstand Requirements," of EPRI TR-107330, with reference to Appendix B, Section 3.5, "Electrostatic Discharge (ESD)," of EPRI TR-102323, Revision 1. EPRI TR-102323 specifies IEC Std 61000-4-2, "Electrostatic Discharge Immunity Test" as an optional test because electrostatic discharge is not considered a common-cause failure mechanism for safety-related systems.

The HFC-6000 platform was subjected to ESD testing using test levels of 8 kV for contact discharge and 15 kV for air discharge applied to specified components of the test specimen. In addition, an 8 kV contact discharge was applied to the vertical coupling plane (VCP) around the perimeter of the test specimen.

TS901-000-25 (Reference 135) provides a summary of the ESD test results. The HFC-6000 did not exhibit any functional susceptibility to the ESD pulses and experienced no permanent damage due to application of the ESD test waveforms. During application of ESD pulses to IOMs, the specific module tested showed no more than two ICL communication errors during application of the pulses. These occurrences had no functional impact on test specimen performance. Thus, the HFC-6000 platform met the acceptance criteria for ESD testing. Based on review of the test procedure and results, the NRC staff concludes that the HFC-6000 platform met the ESD criteria of EPRI TR-107330.

3.3.5.5 Class 1E to Non-Class 1E Isolation Testing

Clause 7.2.2, "Isolation Devices," of IEEE Std 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits," provides the guidance for Class 1E to non-Class 1E isolation that includes the use of isolation devices so that (a) the maximum credible voltage or current transient applied to the device's non-Class 1E side will not degrade the operation of the circuit connected to the device Class 1E or associated side below an acceptable level; and (b) shorts, grounds, or open circuits occurring in the non-Class 1E side will not degrade the circuit connected to the device Class 1E or associated side below an acceptable level.

EPRI TR-107330 includes isolation testing as part of the qualification test sequence and specifies that testing demonstrate an isolation capability of at least 600 VAC and 250 VDC applied for 30 seconds for each module, data acquisition port, and communications port type. In addition to the module to module test levels specified in Section 4.6.4, "Class 1E/Non-1E Isolation Requirements," particular isolation demands and test levels are indicated in the module-specific subsections of Sections 4.3.2, "Input Requirements," and 4.3.3, "Output Requirements," and in Sections 4.3.4.3, "Data Acquisition Requirements," and 4.3.4.4, "Communication Port Requirements," of the EPRI guide. The test levels for channel-to-channel (port-to-port) isolation differ for each module type.

In Sections 8.5.2 and 8.8 of the TR, HFC states the HFC-6000 platform design does not employ isolation devices with the exception of an isolation gateway on the C-Link to provide unidirectional communication to nonsafety-related equipment. This gateway is not part of the HFC-6000 platform scope so no review of the gateway as an isolation device can be performed. Consequently, the scope of the evaluation, as indicated in Section 2.1 of this TR, does not include interconnections with nonsafety equipment. Nevertheless, HFC states that fiber optic cabling for the C-Link network provides electrical isolation for this single interconnection with nonsafety-related equipment that is identified in the TR. Since the electrical-to-optical coupling between the twisted pair wires from the HFC-SBC06 module and the fiber optic physical medium of the C-Link network, which HFC identifies as the ECS-B232 fiber optic transmitter module, is also not within the scope of the platform under review, an evaluation of the Class 1E to non-Class 1E isolation that may be provided by the fiber optic cable remains for a plant-specific review. Therefore, it is an ASAI to confirm that fiber optic cabling is employed for the safety C-Link network and the fiber optic coupling between the HFC-SBC06 modules and the physical medium of the C-Link provides adequate electrical isolation (see Section 5.2 of this SE).

The testing guidance in EPRI TR-107330 specifies isolation testing of main chassis interconnections with expansion chassis as well as communication ports to the controller module (i.e., port to processor interconnection). HFC excluded these interconnections from the isolation tests based on the following considerations (Reference 137). First, interconnections internal to the equipment cabinet are wholly within the Class 1E boundary. Second, external interconnections with the HFC-6000 platform consist solely of ICL fiber optic cabling to any remote chassis and the fiber optic C-Link network among safety nodes. The fiber optic cables provide electrical isolation. Since the HFC-ILR06 fiber optic module is identified as part of HFC-6000 platform, the HFC rationale for excluding the ICL cabling is confirmed by inclusion of the module within the platform scope and is acceptable on the basis of its qualification as part of the test specimen.

The rationale for excluding the communication ports for the C-Link cannot be confirmed since the ECS-B232 module and the physical medium of the C-Link network are not within the scope of the platform under review. Therefore, any interconnection of the HFC-6000 platform with other systems across the C-Link is subject to plant-specific review (see Section 5.2 of this SE).

As indicated in Section 9.3.3.6 of the TR, the primary purpose of these tests was to demonstrate immunity to faults from the inputs to the I/O modules, not to qualify the modules as Class 1E isolation devices. Isolation testing for the HFC-6000 test specimen was performed for the IOM modules as specified in EPRI TR-107330 and the test results are summarized in TS901-000-28 (Reference 136). The module tests for each IOM type were performed with 250 VDC and 600 VAC test signals with some exceptions. Due to limitations of the high potential power test signal source, certain IOM were tested using an alternate test signal source with a capacity of 283 VAC.

The isolation tests demonstrate that no I/O channel other than the channel under test was affected by the test signal and no module other than the module under test was affected by the test signal. Each HFC-6000 IOM successfully demonstrated an isolation capability. Specifically, the HFC-AO8F, HFC-DO8J, HFC-DI16I, and HFC-AI4K modules demonstrated no effects for either the module-to-module or channel-to-channel testing with the 250 VDC and 600 VAC test signals applied. In addition, the AI8M module demonstrated no module-to-module impact with the 250 VDC and 600 VAC test signals applied. These modules met the test criteria specified in EPRI TR-107330 for module-to-module isolation and met or exceeded the channel-to-channel isolation criteria. The discrete input channels on HFC-DC34 demonstrated no channel-to-channel effect with the 250 VDC and 600 VAC test signals applied, which exceeded the channel-to-channel isolation criteria for discrete input channels. Channel-to-channel isolation for the HFC-AI8M module was demonstrated at 250 VDC and 283 VAC. The IEEE TR-107330 specifies a level of 40 volts peak (V_p) for the channel-to-channel isolation of pulse input modules so the HFC-AI8M module exceeded the criteria.

Module-to-module isolation was demonstrated at 250 VDC and 283 VAC for the HFC-DC33, HFC-DC34, and HFC-AI16F modules, which did not satisfy the 600 VAC test criteria for I/O modules specified by IEEE TR-107330 but did indicate the level of isolation provided by these modules. Channel-to-channel isolation was demonstrated at those levels for the discrete input and output channels of the HFC-DC33 module and the discrete output channels of the HFC-DC34 module. The channel-to-channel isolation demonstrated by the input and output channels of the HFC-DC34 module and the discrete input channels of the HFC-DC33 exceeded the EPRI TR-107330 isolation criteria for discrete inputs and 125 VDC outputs. The channel-to-channel isolation demonstrated by the output channels of the HFC-DC33 module did not satisfy the 600 VAC test criteria for 120 VAC output channels but did indicate the level of isolation provided by the discrete output channels on this module. Channel-to-channel isolation was demonstrated at 40 VAC for the HFC-AI16F module, which exceeded the ±30 V_p test criteria for analog inputs specified by EPRI TR-107330.

Therefore, the HFC-AI8M, HFC-AI4K, HFC-DI16I, HFC-AO8F, and HFC-DO8J modules fully satisfy the isolation criteria of EPRI TR-107330. The HFC-DC33, HFC-DC34, and HFC-AI16F modules do not satisfy the module-to-module isolation criteria of EPRI TR-107330 but do provide an isolation capability at 250 VDC and 283 VAC. The discrete input channels of the HFC-DC33 and HFC-DC34 modules, the discrete input channels of HFC-DC33 and the analog input channels of the HFC-AI16F module fully satisfy the channel-to-channel isolation criteria of EPRI TR-107330. The discrete output channels of the HFC-DC33 module do not satisfy the channel-to-channel isolation criteria of EPRI TR-107330 but do provide an isolation capability at 250 VDC and 283 VAC.

Based on the evidence from isolation testing, the NRC staff has determined that the HFC-6000 IOMs provide an acceptable capability for channel-to-channel and module-to-module isolation within a safety division. As noted above, the TR did not identify a role for the HFC-6000 IOMs in the provision of Class 1E to non-Class 1E isolation. Consequently, evaluating the suitability of the IOMs to satisfy regulatory requirements for isolation between safety and nonsafety equipment was not a primary purpose of the review of the isolation test results for the HFC-6000 platform. Nevertheless, the HFC-AI8M, HFC-AI4K, HFC-DI16I, HFC-AO8F, and HFC-DO8J modules have demonstrated an acceptable capability to provide Class 1E to non-Class 1E isolation that satisfies the electrical isolation criteria of EPRI TR-107330 and is consistent with the guidelines contained in Clause 7.2.2 of IEEE Std 384-1992. It is noted that HFC reported damage by the applied voltages to some signal channels under test during the course of isolation testing. Thus, if a specific application requires Class 1E to non-Class 1E isolation to be provided by those qualified HFC-6000 IOMs, then it is an ASAI to confirm that the qualification envelope for the specific module(s) employed to provide electrical isolation bounds the maximum credible voltages applied to the interconnected non-Class 1E equipment and it must also be demonstrated that the execution of the safety function implemented using the HFC-6000 platform will be unaffected by loss of the I/O capability of any of those modules due to damage while providing electrical isolation (see Section 5.2 of this SE).

3.3.6 Seismic Withstand Testing

Clause 4, "Seismic Qualification Approach," of IEEE Std 344-1987, "IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations," states that the seismic qualification of Class 1E equipment should demonstrate an equipment's ability to perform its safety function during and after the time it is subjected to the forces resulting from one SSE. In addition, the equipment must withstand the effects of a number of operating basis earthquakes (OBEs) prior to the application of a safe shutdown earthquake (SSE). The guidance for seismic withstand testing that the HFC-6000 platform is required to satisfy is given in Section 6.3.4, "Seismic Test Requirements," of EPRI TR-107330. Section 4.3.9, "Seismic Withstand Requirements," of the EPRI guide specifies the required response spectrum (RRS) for the OBEs and SSE as 9.75 g and 14 g, respectively, based on 5 percent horizontal and vertical damping.

Seismic testing exposed the HFC-6000 test specimen to a set of dynamic spectra designed to simulate an OBE and a SSE. The dynamic spectra consisted of tri-axial, random, multi-frequency waveforms that were transmitted to the test specimen by means of hydraulic actuators attached to a seismic simulator table at Wyle Laboratories. The test specimen was subjected to inspection and performance testing before and after the seismic testing. During the conduct of the seismic withstand test program, the test specimen was subjected to a low amplitude resonance search to identify critical frequencies below 100 Hz, five OBE tests, and one SSE test. However, because of limitation of the seismic simulator table, the maximum seismic acceleration that could be achieved during the SSE test was 10 g.

3.3.6.1 Resonance Search Test

As specified in EPRI TR-107330, a resonance test was conducted to identify any resonant frequencies for test specimen components within the RRS. The test was conducted by imposing a low level sinusoidal sweep. As reported in Section 9.3.3.5 of the TR, the resonance frequencies detected by the sweep were used to establish the test response spectrum (TRS) that would produce the maximum response in the test specimen. The NRC staff finds that the resonance search test approach complies with the guidance of EPRI TR-107330 and is, therefore, acceptable.

3.3.6.2 Qualification-Level Multiple-Frequency Tests

The sequence for seismic dynamic testing is specified in EPRI TR-107330, Section 6.3.4. The dynamic seismic tests performed by HFC consisted of five tests based on the OBE RRS and one test based on the SSE RRS. The response spectrum of the test specimen was reported for 0.5 percent, 1.0 percent, 2.0 percent, 3.0 percent, and 5.0 percent damping factors. During each dynamic test, automated operability and prudency tests were executed to verify overall system performance. Following each dynamic test, the entire test specimen was examined for mechanical damage. Any mechanical damage sustained during testing was recorded. The detailed test results are documented in TS901-000-35, "Seismic Testing Summary Report" (Reference 138). TN901-000-07 (Reference 132) and TN901-000-12 (Reference 133) provide updates and corrections to the test summary based on further analysis of the seismic test results.

The initial seismic test was run after completion of the surge withstand test. HFC decided to repeat the entire seismic test because the test specimen experienced several anomalies, including a fault in the data recorder, which resulted in incomplete data. Prior to the seismic retest, all damaged modules were replaced or repaired. Additionally, all operability and prudency tests were repeated at HFC facilities prior to reshipment to Wyle Laboratories. The results of the seismic testing in-house testing are reported in TS901-000-34 (Reference 124) and are discussed in Section 3.3.2 of this SE.

As stated in Section 9.3.3.5 of the TR, HFC concluded that the results of repeated dynamic seismic tests showed the test specimen successfully withstood the stress and continued to function normally. During one of the OBE tests, a power supply assembly in the PSM came partially out of the rack. Power to the test specimen was not lost and the test was successfully executed. However, HFC installed a locking bar on the PSM rack to the power supply assemblies to ensure the seismic withstand capability is maintained. It is an ASAI to confirm that the locking bar is installed for fielded systems based on the HFC-6000 platform (see Section 5.2 of this SE). Other reported anomalies were evaluated by HFC and determined to be either unrelated to the imposition of seismic acceleration stress or indicative of the robustness provided by the redundant components of the HFC-6000 platform.

Table 5.1 of EPRI TR-107330 specifies that all operability and prudency tests are to be executed during the SSE test. Thus, test results for the SSE test should address the acceptability of the performance characteristic covered by the functional tests. Based on review of the test summary documents, it was determined by the NRC staff that the test results do not report data for each performance criterion specified in EPRI TR-107330. To resolve this documentation deficiency, HFC submitted TS901-000-44, "ERD111 Seismic Qualification Analysis Report" (Reference 139), to more comprehensively document the seismic test findings and to provide supporting analysis. Since data was not available for every performance characteristic addressed by the operability and prudency tests, HFC provided additional analysis to supplement the evidence of qualification by type test. This approach conforms to the third acceptable method of seismic qualification provided by IEEE Std 344-1987 (i.e., qualify the equipment by a combination of test and analysis).

Based on a review of the test results and supporting analysis, the NRC staff determined that the HFC-6000 platform does not fully satisfy the guidance of EPRI TR-107330 because seismic withstand was not demonstrated for the specified maximum acceleration (14 g) for a generic SSE. However, the NRC staff finds that seismic qualification of the HFC-6000 platform has been acceptably demonstrated for OBE and SSE events up to 10 g. It is an ASAI to confirm that the qualified seismic withstand capability of the HFC-6000 platform bounds the plant-specific seismic withstand requirements (see Section 5.2 of this SE).

3.4 Platform Integrity Characteristics

SRP Chapter 7, Appendix 7.1-C, Section 5.5, "System Integrity," states that a special concern for digital computer-based systems is confirmation that system real time performance is adequate to ensure completion of protective actions within the critical time periods identified as required by Clause 4 of IEEE Std 603. SRP BTP 7-21, "Guidance on Digital Computer Real-Time Performance," provides supplemental guidance on evaluating response time for digital computer-based systems, and discusses design constraints that allow greater confidence in analyses of results or prototype testing to determine real time performance. In summary, the integrity of a safety system is given evidence by a predictable response time, which in turn depends on deterministic behavior and fault management capabilities in addition to the timing characteristics of the hardware/software system.

3.4.1 Response Time

The accident analysis of design basis events at nuclear power plants includes a determination of how soon the protective actions are needed to mitigate those design basis events. The regulations that contain the basis for this requirement are in 10 CFR 50.55a(h). In addition, 10 CFR 50.36(c)(1)(ii)(A) requires inclusion of the limiting safety systems settings for nuclear reactors in the plant technical specifications (TSs), with those settings "so chosen that automatic protective action will correct the abnormal situation before a safety limit is exceeded." Once the total time required for a protective action has been determined, licensees allocate portions of that time to elements of the protective system (i.e., the time required for the sensors to respond to changes in plant conditions, the time required for the actuation logic, and the time required for a valve to close or a pump to start).

GDC 20, 21, 23, and 25 (of Appendix A to 10 CFR Part 50) constitute general requirements for timely operation of the protection features. To meet these requirements, SRP BTP 7-21 provides the following guidance:

- The feasibility of design timing may be demonstrated by allocating a timing budget to components of the system architecture so that the entire system meets its timing requirements.
- Timing requirements should be satisfied by design commitments.

Section 4.2.1, Item A of EPRI TR-107330 states "The overall response time from an input to the PLC exceeding its trip condition to the resulting outputs being set shall be 100 milliseconds or less." To establish qualification of a generic PLC platform, Section 5.3, "Operability Test Requirements," Part B, "Response Time" states that the "response time between receiving a discrete input and setting a discrete output and from changing an analog input to changing an AO and a discrete output shall be measured in a fashion that is expected to provide repeatable results." Specifically, the EPRI guide states that determination of the response time should address the effect of input filtering, the I/O data acquisition time (e.g., sampling, conversion, etc.), the input access time for bus transfer to the main processor, twice the execution cycle time for an application program containing the equivalent of 20M simple logic elements, the output access time for bus transfer to I/O cards, and the I/O data distribution time. The EPRI TR-107330 specifies that the response time of the PLC platform also includes the maximum time required to invoke any diagnostic and redundancy features (e.g., redundant processor synchronization, inter-processor communication, and diagnostic routine execution).

In its response to RAI Part 3 (Reference 17), HFC defined the maximum response time characteristics of the HFC-6000 platform in terms of the worst-case response to I/O changes. As described by HFC, the calculation of the total platform response time consists of five separate time periods:

- The scan time (*T1*) required for an AI or DI module to read and process its inputs.
- The scan time (*T2*) required for the controller to fetch the input data from an AI or DI module.
- The time required for the controller to execute the application program (*T3*).
- The scan time (*T4*) required for the transfer of the output data to the AO or DO module, with the duration of *T4* is equal to that of *T2*.
- The scan time (*T5*) required for updating the output channel signal status.

The primary activities that embody the scan time elements identified above involve the IOM performing data scans nominally every 10 ms, the ICL processor sequentially polling the IOM on a fixed interval as part of the cyclic execution of its primary task, and the SYS processor executing the application program at least once every context switch interval (e.g., 50 ms or 100 ms). With the data exchange between the ICL and SYS processors involving buffered interaction through loosely coupled access to shared memory, these scan activities are executed asynchronously. Given deterministic performance of the platform, each of the contributing time intervals, for any particular system configuration, is essentially fixed from one processing cycle to the next cycle (i.e., variations on the order of milliseconds). Consequently, HFC identifies the theoretical best-case response time as the sum of the five time intervals defined above and the worst-case response time as twice this value. The diagnostic and redundancy feature execution times of the HFC-6000 platform are included in the normal execution cycle within a context switch interval so the HFC scan time elements address the response time contributors specified in EPRI TR-107330. Based on its review of the cited documents, the NRC staff finds that the HFC approach for evaluating the response time of the HFC-6000 platform is consistent with the guidance of EPRI TR-107330 and is, therefore, acceptable.

The operability tests of the HFC-6000 test specimen under the ERD111 qualification project provided indication of the response time performance for a fully loaded system with high levels of I/O activity. The extensive functionality implemented in the TSAP (Reference 110) served as a high-end example of the computational and I/O scanning demands that can be supported by the platform. In Section 8.1.2 of the TR, HFC committed to perform a plant-specific timing analysis to demonstrate deterministic performance and ensure that response time requirements are met.

During the environmental qualification baseline testing, the HFC-6000 test specimen demonstrated digital response times that averaged less than 110 ms, with a range from 60 ms to 176 ms. The demonstrated analog response times were greater than 1 second. As described in TS901-000-22 (Reference 92), the investigation of those results by HFC indicated that the dynamic response of the input filtering for the HFC-AI16F module and the effect of signal processing (i.e., 100-sample moving average algorithm) on the AI data acquisition were significant factors in the unacceptable performance. As part of the corrective action response, the input filter capacitors were changed to reduce the transfer time upstream of the ADC on the module. In addition, the operating software of the IOM underwent maintenance modification to correct the response time performance deficiency. The software maintenance consisted of changing the parameters for the signal-processing algorithm so that it provided 2-sample averaging rather than 100-sample averaging. Thus, this maintenance modification did not introduce new functionality but instead tuned the performance to address the requirement. During regression testing, it was confirmed that the modified HFC-AI16F module was able to support response times more suitable for safety applications.

Subsequently, HFC evaluated response time capabilities through baseline testing for the HFC-6000 platform. The response time tests were conducted using the HFC-6000 test specimen executing the TSAP synthetic application code and consisted of simulated setpoint crossings via a square wave test signal to trigger trip outputs. The test results demonstrated maximum response times of 380 ms for an analog input (HFC-AI16F) to digital output (HFC-DO8J) signal path and 180 ms for a digital input (HFC-DI16I) to digital output (HFC-DO8J) signal path. The testing covered several configurations of the TSAP, based on code optimization and minimized processor loading (i.e., reduction of the TSAP functional scope to address only response time testing). The analog response times observed in testing ranged from 160 ms to 380 ms, with the reduced application code cases ranging from 160 ms to 220 ms and the fully loaded cases ranging from 200 ms to 380 ms. The observed digital response times ranged from 30 ms to 180 ms. HFC did not evaluate or test the response time characteristics of other input-to-output signal path combinations.

On the basis of the measured response times for the baseline testing, the HFC-6000 platform is not in compliance with Section 4.2.1, Item A of EPRI TR-107330. However, the actual response time for any particular system will depend upon the specific system configuration and required functionality of the application software. Thus, the response time for any particular implementation of the HFC-6000 platform may vary significantly from simple to complex systems. Based on the review of the HFC response time test results and consideration of the dependence of the actual response time for a system on its application-specific configuration, the NRC staff has determined that the response time characteristics are suitable to support safety-related applications in nuclear power plants. However, confirmation of the acceptability of system response time based on timing analyses and functional testing for a particular application implementation and system configuration is an ASAI and is, therefore, the responsibility of licensees (see Section 5.2 of this SE). The response time performance of a safety-related system based on the HFC-6000 platform is subject to plant-specific review to ensure that it satisfies its plant-specific and application-specific requirements for system response time presented in the accident analysis in Chapter 15 of the safety analysis report for the plant.

3.4.2 Deterministic Performance

In SEP Chapter 7, Appendix 7.1-C, Section 6.1, "Automatic Control," the review guidance identifies considerations for addressing digital computer-based systems in the evaluation of the automatic control capabilities of safety system command features. Specifically, it is advised that the evaluation should also confirm that the system's real-time performance is deterministic and known. In addition, SRP BTP 7-21 discusses design practices for computer-based systems that should be avoided. These practices include non-deterministic data communications, non-deterministic computation, use of interrupts, multitasking, dynamic scheduling, and event-driven design. The technical position further states that methods for controlling the associated risk to acceptable real-time performance should be described when such practices are employed.

EPRI TR-107330 includes requirements intended to achieve deterministic execution cycle behavior such that an application and its constituent tasks will be completely executed within a specific time frame. In particular, Section 4.4.1.3, "Program Flow Requirements," specifies that, for those PLCs where scanning of the inputs and application program execution are performed in parallel, the PLC executive must provide methods for assuring that both the input scan and application program execution are completed each cycle. In effect, the EPRI guide specifies a continuous, essentially non-interruptible, software architecture as the preferred software environment for safety functions.

[

]

Evaluation of the deterministic performance characteristics of the HFC-6000 requires consideration of the multitasking environment, application execution cycle, interrupt usage, and communications capabilities. As discussed in Sections 3.1.3.2.1 and 3.1.3.2.2 of this SE, the OS of HFC-6000 platform provides an execution environment in which multiple tasks, each executing independently of the other tasks, can be invoked by the OS based on sequential scheduling or time-based scheduling. [

] Therefore, the NRC staff concludes that the HFC-6000 platform provides acceptable deterministic performance characteristics and it is suitable to support a safety-related application in a nuclear power plant when appropriately implemented.

3.4.3 Diagnostics and Self-Test Capabilities

SRP BTP 7-17, “Guidance on Self-Test and Surveillance Test Provisions,” states that automatic diagnostics and self-test features should preserve channel independence, maintain system integrity, and meet the single-failure criterion during testing. Additionally, the benefits of diagnostics and self-test features should not be compromised by the additional complexity that may result from their implementation. In particular, the scope and extent of interfaces between safety software and diagnostic software such as self-test routines should be designed to minimize the complexity of the integrated software.

EPRI TR-107330 specifies that the PLC platform must provide sufficient diagnostics and test capability so that a combination of self-diagnostics and surveillance testing will detect all failures that could prevent the PLC from performing its intended safety function. The range of conditions for which diagnostics or test capabilities must be provided includes processor stall, executive program error, application program error, variable memory error, module communications error, module loss of configuration, failure feature to detect excess scan time, application not executing, and field device (i.e., sensor, actuator) degradation or fault. The means of detection identified include watchdog timer, checksum for firmware and program integrity, read/write memory tests, communications monitoring, configuration validation, heartbeat, and self-diagnostics or surveillance test support features. Both online and power-up diagnostics are specified.

The HFC-6000 platform provides online diagnostics and continuous self-testing, including checking memory, monitoring processor status, validating communication links, and using watchdog timers (References 47, 48, and 49). [

]

The NRC staff has reviewed the diagnostics and self-test capabilities for the HFC-6000 platform, and finds them to be suitable for a digital system used in safety-related applications in nuclear power plants. The diagnostics capabilities are found to be adequate, in combination with a regular surveillance program, to provide the detection capabilities claimed in the failure modes and effects analysis (Reference 141) conducted by HFC for a representative system configuration based on the HFC-6000 platform (see Section 3.8.2.1 of this SE). The NRC staff has determined that the diagnostics and self-test capabilities comply with the guidance of EPRI TR-107330 overall. The NRC staff concurs with the rationale provided by HFC in RR901-000-10, "EPRI TR 107330 Requirements Compliance Traceability Matrix" (Reference 137), regarding the exceptions taken to providing power-up diagnostics for features that require a runtime environment. In addition, the NRC staff accepts the HFC position that regular surveillance testing is necessary, in addition to the diagnostics and self-test capabilities of the HFC-6000 platform, to detect some of the failures identified in the EPRI guide and in the failure modes and effects analysis discussed in Section 3.8.2.1.

3.5 Communications Independence

IEEE Std 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 nonsafety system, a logical or software malfunction of the nonsafety system must not be able to affect the functions of the safety system.

IEEE Std 7-4.3.2-2003, endorsed by RG 1.152, Revision 2, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Clause 5.6, "Independence," provides guidance on how IEEE 603 requirements can be met by digital systems. This clause of IEEE Std 7-4.3.2 states that, in addition to the requirements of IEEE Std 603-1991, data communication between safety channels or between safety and nonsafety systems shall not inhibit the performance of the safety function. SRP Chapter 7, Appendix 7.1-D, Section 5.6, "Independence," provides acceptance criteria for computer equipment qualification. This section states 10 CFR 50, 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. Additional guidance on interdivisional communications is contained in "Interim Staff Guidance, Digital Instrumentation and Controls, DI&C-ISG-04, Task Working Group #4, Highly-Integrated Control Rooms Communications Issues (HICRc)." DI&C-ISG-04 compliance is discussed further in Section 3.5.2.

The NRC staff reviews the overall design of a safety-related system. As part of this review, the NRC staff evaluates applicability and compliance with SRP Section 7.9, "Data Communication Systems," SRP Chapter 7, Appendix 7.0-A, "Review Process for Digital Instrumentation and Control Systems," and SRP BTP 7-11, "Guidance on Application and Qualification of Isolation Devices." SRP BTP 7-11 provides guidance for the application and qualification of isolation devices, and applies to the use of electrical isolation devices to allow connections between redundant portions of safety systems or between safety and nonsafety systems.

The evaluation includes a review to determine if a malfunction in one portion affects the safety functions of the redundant portion(s) because signal communications may exist between different portions of the safety system. The evaluation includes a review to determine if a logical or software malfunction of the nonsafety system affects the functions of the safety system since the safety system can be connected to a digital computer system that is nonsafety.

3.5.1 Communications Interconnections

The communications interfaces for the HFC-6000 platform are described in Section 3.1.2 of this SE. In addition, the protocol software is described in Sections 3.1.3.2.3 and 3.1.3.2.4 of this SE. The deterministic characteristics of the communication functions provided by the HFC-6000 platform are described in Section 3.4.2 of this SE. The two means of digital communications interconnections are the ICL and the C-Link. [

]

Based on the review of communications interfaces and protocols described above and in Sections 3.1.2, 3.1.3.2.3, and 3.1.3.2.4 of this SE, the NRC staff has determined that execution of a safety function on the SYS processor of the HFC-SBC06 controller module is appropriately isolated from transaction management functions for network communications based in the use of interposing processors (i.e., C-Link and ICL processors) and the use of shared memory to exchange communicated data and messages among processors. Coupled with the evaluation of deterministic performance characteristics of these communications capabilities in Section 3.4.2 of this SE, the NRC staff concludes that the communications capabilities provided by the HFC-6000 platform (that are within the scope of the TR) are suitable to support safety-related applications in nuclear power plants when appropriately implemented for communications interconnections.

3.5.1.1 Communications from HFC-6000 Platform to Other Safety-Related Equipment

The communications interconnections established between a safety division and other safety-related equipment in a plant are solely dependent on the safety system design. The base architecture presented for the HFC-6000 platform is representative of a single division or channel in a safety system and the interconnection with other systems is a plant-specific determination. Since the TR does not address a specific application, establish a definitive safety system design, nor identify any plant I&C architectures, no evaluation of the communications from the HFC-6000 platform to other safety-related equipment, including other HFC-6000 platforms, could be performed.

3.5.1.2 Communications with Nonsafety Systems

Determination of communications interconnections between a safety system and other nonsafety systems in a plant is an application-specific activity. The base platform architecture identified in the TR does not specify any direct connections or bi-directional communication between the HFC-6000 and any other system. However, the TR does identify the capability for one-way communication to nonsafety-related components across the C-Link network though fiber optic cabling and an isolation gateway. To promote independence, HFC established a design principle for nuclear safety applications that restricts communication over the C-Link network to broadcast-only messages so peer-to-peer communication is not allowed (Reference 21). The gateway and network medium are not part of the base platform and thus are not within the scope of the review. Since the TR does not address a specific application or system configuration and any potential unidirectional interconnection with nonsafety systems through an isolation gateway is outside the scope of the platform, no evaluation of the communications from the HFC-6000 platform with nonsafety systems could be performed. It remains an ASAI to verify that peer-to-peer communication is not implemented as part of the online capabilities of the plant-specific design and that any device (e.g., gateway) installed as a node on the C-Link as an interface to nonsafety systems or networks is restricted to unidirectional communication (i.e., receive only) and does not transmit across the C-Link (see Section 5.2 of this SE).

3.5.1.3 Communications Between Separate Class 1E Divisions

The redundant configuration of a multi-divisional safety system and the independence provided between those redundant divisions are solely dependent on the safety system design. The base architecture presented for the HFC-6000 platform is representative of a single division or channel in a safety system. Since the TR does not address a specific application, establish a definitive safety system design, nor identify any plant I&C architectures, no evaluation of the communications between separate Class 1E divisions could be performed.

3.5.2 Staff Guidance in DI&C-ISG-04

The NRC Task Working Group #4, "Highly Integrated Control Rooms-Communications Issues," has provided interim NRC staff guidance on the review of communications issues. DI&C-ISG-04 contains three sections, (1) Interdivisional Communications, (2) Command Prioritization, and (3) Multidivisional Control and Display Stations. The guidance provides "requirements for separation, independence, electrical isolation, seismic qualification, quality requirements, etc. cited in the General Design Criteria of Appendix A to Part 50 of Title 10 of the *Code of Federal Regulations*."

3.5.2.1 DI&C-ISG-04, Section 1 - Interdivisional Communications

Section 1 of DI&C-ISG-04 provides guidance on the review of 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. This ISG does not apply to communications within a single division.

The TR does not provide a specific safety system design nor does it address interdivisional communications. In the HFC response to RAI Part 3 (References 17 and 18), HFC staff indicated that one means of providing interdivisional communication is via hardwired unidirectional links using I/O modules on the ICL bus. However, the specific I/O modules were not identified and this configuration was not addressed within the scope of the base platform. Thus, interdivisional communications could not be evaluated at the platform level but remains subject to a plant-specific review.

The C-Link networking capability for the HFC-6000 platform is restricted to intra-divisional broadcast-only communication among safety controller nodes. Specifically, HFC design practice for safety applications is to prohibit direct peer-to-peer communication with or among the CPUM on the C-Link network (Reference 21). However, the C-Link network is also designed to support unidirectional communication from safety controllers within a division to nonsafety-related equipment. This communication capability is described in Sections 6.1, 7.2.1, and 8.9 of the TR. As described, the C-Link enables broadcast of the DDB, which contains data and status information from each controller within a single division. Although the TR describes the use of a gateway device to enforce one-way communication to transmit the broadcast operational data/information to nonsafety system(s), the gateway is not included within the platform scope so it cannot be reviewed at the platform level. The provision of strictly unidirectional communication (i.e., receive only) by a gateway device is an ASAI that will be reviewed in the context of a specific application (see Section 5.2 of this SE). In addition, adherence to the design principle that prohibits peer-to-peer communication on the safety C-Link network is an ASAI that is subject to plant-specific review (see Section 5.2 of this SE).

3.5.2.2 DI&C-ISG-04, Section 2 - Command Prioritization

Section 2 of DI&C-ISG-04 provides guidance applicable to a prioritization device or software function block, which receives device actuation commands from multiple safety and nonsafety sources, and sends the command having highest priority on to the actuated device.

The design of field device interfaces and the determination of means for command prioritization are application-specific activities. Since the TR does not address a specific application, no evaluation against this NRC staff position could be performed.

3.5.2.3 DI&C-ISG-04, Section 3 - Multidivisional Control and Display Stations

Section 3 of DI&C-ISG-04 provides 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, and 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.

The design of information displays and operator workstations and the determination of information sources and interconnections are application-specific activities. Since the TR does not address a specific application nor include display devices within the scope of the platform, no evaluation against this NRC staff position could be performed.

3.6 Secure Development and Operational Environment

RG 1.152, Revision 2, describes a method that the NRC deems acceptable for complying with the Commission's regulations to promote high functional reliability, design quality, and security for the use of digital computers in safety-related systems at nuclear power plants. Specifically, the guidance for secure development and operational environment measures states that security vulnerabilities should be addressed in each phase of the digital safety system life cycle. The overall guidance provides the basis for physical and logical access controls to be established throughout the digital system development process to address the susceptibility of a digital system to inadvertent access. [Note: Although Revision 2 of RG 1.152 does contain language addressing cyber security and malicious threats, 10 CFR 73.54 and its guidance now address cyber security for licensees. Thus, this evaluation does not make any conclusions regarding the HFC-6000 platform's ability to withstand cyber attacks. Protection from cyber threats will need to be addressed by licensees under the cyber security programs, as required by 10 CFR 73.54.]

RG 1.152 utilizes the waterfall life cycle phases defined for the development of a high quality safety-related system as a framework for establishing digital system secure development and operational environment guidance and establishing criteria for acceptability. The identified life cycle structure, for which criteria on development environment controls are to be established, consist of the following phases:

- Concepts
- Requirements
- Design
- Implementation
- Test
- Installation, Checkout, and Acceptance Testing
- Operation
- Maintenance
- Retirement

This SE presents findings based on regulatory positions 2.1 through 2.5 (i.e., the development phases, Concepts through Test) for the HFC-6000 platform. The phases covered by regulatory positions 2.6 through 2.9 of RG 1.152 (i.e. Installation, Checkout, and Acceptance Testing; Operation; Maintenance; and Retirement phases) are heavily dependent on licensee responsibilities for an application-specific system within a plant-specific context. In the absence of a specific application, the evaluation can only address the platform-level features and characteristics that are relevant for maintaining a secure operational environment.

In addition, the operating software of the HFC-6000 platform was developed prior to the issuance of Revision 2 of RG 1.152. Thus, the discussion of development activities is focused on those secure development environment considerations applied during the CGD effort and that will apply to the life cycle processes related to the maintenance of the PDS. Although application software is not within the scope of this review, platform features that contribute to a secure operational environment for the application are identified and discussed. Credit may be taken for the use of these security capabilities in establishing a secure operational environment for a plant-specific safety-related application.

3.6.1 Concepts Phase

3.6.1.1 Platform Security Capabilities

As stated in the regulatory position 2.1 of RG 1.152, Revision 2, the concepts phase is when the developer identifies security capabilities for a safety-related system that are to be implemented. However, the HFC-6000 platform was developed prior to the issuance of this regulatory guidance in 2006. Thus, the security-enabling capabilities of the HFC-6000 platform were not instituted to fulfill an explicitly articulated security concept but rather were the product of good design practices. HFC has documented a security concept to identify the security capabilities of the platform design. This security concept is contained in RR901-000-23 (Reference 28). The HFC security concept addresses hardware and software features of the platform as well as the approach for maintaining existing software and developing new software [Note: application software development is not evaluated in this SE.]. In addition, the security concept addresses platform failure modes that are relevant to inadvertent access, measures to detect and respond to those failures, and specific automatic diagnostics and self tests that support secure operations during initialization and operation of the platform.

[

] The security capabilities that are identified were used to establish the security requirements for the platform hardware and software, which are addressed in Section 3.6.2.1 of this SE. Although development of the HFC-6000 platform preceded the issuance of RG 1.152, Revision 2, the NRC staff review has concluded that the security concept defined in RR901-000-23 and the platform capabilities identified in that document comply with this criterion from regulatory position 2.1 regarding identification of safety system security capabilities.

3.6.1.2 Identification of Life Cycle Vulnerabilities

Regulatory position 2.1 of RG 1.152, Revision 2, also states that potential security vulnerabilities should be identified by the developer based on performance of a security assessment covering each phase of the system life cycle. The results of the assessment form the basis for establishing security requirements for the system (hardware and software).

Again, because the development of the HFC-6000 predated the issuance of the security guidance in RG 1.152, Revision 2, HFC did not perform a formal security assessment during the initial development of the product line. However, the HFC software QA program explicitly addresses security (see Sections 3.2.2.9 and 3.2.2.10.1 of this SE) through the required treatment of secure operational environment considerations in a requirements assessment specified as an action within of the SSP and by the SVVP requirement that a security analysis be performed at each software life cycle phase, in addition to criticality, hazard, and risk analyses.

In addition, HFC has provided findings from security vulnerability analyses in their summary responses to clarifying inquiries that were posed within the acceptance letter for the TR (Reference 14) and in their revised response to RAI Part 3 (Reference 18).
[

]

Given the fact that the HFC-6000 platform was an existing design when Revision 2 of RG 1.152 was released, the NRC staff finds the post-development analysis to be acceptable under the prevailing circumstance.

Based on review of the vulnerabilities identified in the security analyses performed by HFC, the NRC staff found the platform-level assessment of security vulnerabilities from the concepts phase through the test phase, with additional consideration of vulnerabilities during the operation phase, to be acceptable and suitable for reference in application-specific security analyses. Specifically, the NRC staff finds that these identified vulnerabilities adequately address the potential for tampering with the HFC-6000 platform during the developmental phases associated with either maintenance of PDS or configuration of the platform to support an application. The vulnerabilities identified in the analyses contribute to the basis for security functional requirements for the platform, which are discussed in Section 3.6.2.1 of this SE, and support the determination of appropriate security controls for system hardware and software development, which are described in Sections 3.6.2.4, 3.6.3.3, 3.6.4.2, and 3.6.5.2 of this SE. Based on the NRC staff's review of the vulnerabilities identified and recognition that process and platform requirements to address these vulnerabilities through the various life cycles have been established, the NRC staff has determined that HFC has met the criterion of regulatory position 2.1 in RG 1.152 for the HFC-6000 platform.

3.6.1.3 Remote Access and One-Way Communication

The guidance in regulatory position 2.1 of RG 1.152 states that implementation of remote access to a safety-related system should not be allowed. In addition, any transfer of data to other systems by computer-based safety-related systems should be limited to one-way communication pathways.

As previously noted, the TR does not address a specific application, establish a definitive safety system design, nor identify any plant I&C architectures so this criterion cannot be fully evaluated. In Section 2.1 of this SE, it is observed that no interconnections with other systems, either safety-related or nonsafety-related, are included within the scope of the platform. In addition, not only does the platform description provided by HFC in the TR clearly indicate that remote access is not intended as a safety design configuration, but the security-informed design principles identified in WI-ENG-020 (Reference 83) specify that design usage of remote access should be avoided. The HFC Security Concept document (RR901-000-23, Revision A) provides a more firm commitment to prohibiting remote access and two-way communications when it states, [

] Although any final determination on remote access and communication with other systems will need to be made on an application-specific basis, based on these considerations, the NRC staff finds that the HFC-6000 platform supports compliance with this criterion of regulatory position 2.1 in RG 1.152.

3.6.2 Requirements Phase

3.6.2.1 Security Functional Performance Requirements

Regulatory position 2.2.1 of RG 1.152 states in part that developers should define security functional performance requirements and system configuration for a safety-related system. Security requirements for interfaces external to the system should be established by the developers as well. Also, the developers should address security requirements for qualification, human factors engineering, data definitions, documentation the software and hardware, installation and acceptance practices, operation and execution conditions, and maintenance activities.

Based on the security analyses discussed above, the HFC-6000 security concept, as documented in RR901-000-23, identifies secure operational environment features of the platform that are traceable to functional performance requirements contained in the SRS for the HFC-6000 platform (References 95, 103, 104, and 105). The secure operational environment functional performance requirements identified in the security concept document can be expressed in terms of specific capabilities of the platform (References 28 and 142). These capabilities include the following features, characteristics, and design elements:

[

]

The requirements implicit in the features and characteristics stated above are embedded in the SRS for the HFC-6000 platform. These features form the basis for the system secure operational environment design that is discussed in Section 3.6.3 of this SE. Based on the review of the reconstituted SRS (as discussed in Section 3.2.3.1 of this SE), giving consideration to the secure operational environment capabilities provided by the features identified above, and recognizing that the remaining items identified in the criterion primarily relate to a system-specific implementation of the platform for a particular application, the NRC staff determined that the HFC-6000 platform has met the criterion of regulatory position 2.2.1 in RG 1.152.

3.6.2.2 Security Requirements V&V

Regulatory position 2.2.1 of RG 1.152 also states that security requirements should be included within the overall system requirements. Therefore, the system security requirements should be subject to treatment under the full V&V process activities of the overall system to assure the correctness, completeness, accuracy, testability, and consistency of those security requirements.

As noted in Section 3.2.2.10.1 of this SE, WI-ENG-022 requires a security analysis be conducted at every phase of the software life cycle as part of the V&V process applied to a development project. RR901-000-38, "Security Overview" (Reference 142), provides a traceability matrix to establish the relationship between security requirements identified in the security concept (Reference 28) and the requirements for platform features specified in the SRS. Consequently, the V&V process applied to the dedication of PDS was shown to address security requirements. Based on these considerations and the review of the HFC V&V program discussed in Section 3.2.2.10 of this SE, the NRC staff finds that the HFC-6000 platform has met the criterion of regulatory position 2.2.1 in RG 1.152.

3.6.2.3 Use of Predeveloped Software and Systems

Regulatory position 2.2.1 of RG 1.152 further states that the security vulnerability of a safety-related system should be addressed in any requirements specifying the use of pre-developed software and systems (e.g., reuse of software and incorporation of commercial off-the-shelf systems). In particular, the use of pre-developed software functions that have been tested and are supported by operating experience is identified.

The predeveloped operating software of the HFC-6000 platform underwent dedication for use in safety-related applications. As described in Section 3.2.1 of this SE, the dedication process indicates the quality and reliability of the PDS is acceptable. In addition, testing and code inspection as part of the CGD effort further establish the quality and security characteristics of the PDS (particularly in relation to the identification of undocumented or unnecessary code). The dedicated operating software is controlled under the HFC SCMP and is maintained under the HFC software QA program. Section 10.1.4 of the HFC TR provides appreciable evidence on the reliable operation of the HFC-6000 platform and its predecessor product lines which used the PDC software. Based on the review of the CGD evidence for the PDS and its ongoing management under HFC quality processes, the NRC staff concludes that the HFC-6000 platform has satisfied this criterion of regulatory position 2.2.1 in RG 1.152.

3.6.2.4 Requirements Phase Development Activities

The regulatory position in Section 2.2.2 of RG 1.152, Revision 2, states, "The development process should ensure the system does not contain undocumented code (e.g., back door coding), malicious code (e.g., intrusions, viruses, worms, Trojan horses, or bomb codes), and other unwanted and undocumented functions or applications." As was covered earlier in Section 3.6.1.2, [

]

As described in the HFC-6000 security concept, RR901-000-23, the HFC software QA program addresses the design, implementation, and commissioning of safety-related systems based on the HFC-6000 platform. The program provides for measures to ensure the maintenance of records. In particular, the HFC software QA program provides guidance through the software security WI, WI-ENG-020. The engineering procedures captured in WI-ENG-020 provide development activity requirements for each life cycle phase. Relative to the requirements phase products, WI-ENG-020 specifies that all documents from every life cycle phase – including requirements documentation – are stored in the repository of documentation control. The second regulatory audit (Reference 16) observed the HFC configuration management controls placed on their documentation products.

In addition, Section 3.2.3.1 of this evaluation addresses the HFC-6000 software requirements specification and Section 3.2.2.10.3 addresses the requirements traceability matrix. Section 3.2.2.11 of this evaluation addresses the HFC configuration management plan for the HFC-6000, which includes control of the software documentation.

[ ] the NRC staff finds that the HFC-6000 platform meets the provisions of Section 2.2.2 of RG 1.152, Revision 2.

3.6.3 Design Phase

3.6.3.1 Security Design Configuration Items

Regulatory position 2.3.1 of RG 1.152 states in part that the safety-related system security requirements included within the SRS should be translated into specific design configuration items in the system design description. [ ]

For life cycle development incorporating this guidance, the design phase involves translation of system secure operational environment requirements into design configuration items. Since the HFC-6000 platform was developed prior to the issuance of this security guidance, this phase corresponds to identification of design configuration items embodied in the realized platform design. As discussed above, the secure operational environment requirements for the HFC-6000 platform correspond to security-related features, capabilities, and design elements that serve as design configuration items.

Regarding access to system functions, physical design configuration items primarily depend on plant-specific system architectures and installation conventions. Logical access involves control of the means to affect software and data within the platform and is discussed in the next section.

[

] Based on these considerations and reviews of platform integrity characteristics and communications independence in Sections 3.4 and 3.5, respectively, of this SE, the NRC staff determined that the HFC-6000 platform has met the criterion of regulatory position 2.3.1 of RG 1.152.

3.6.3.2 Security Design Access Control

Regulatory position 2.3.1 of RG 1.152 also states that qualitative risk analyses addressing security should be performed to provide the basis for physical and logical access control. Security risk is considered to be the combination of the consequence to the nuclear power plant and the susceptibility of a digital system to both internal and external cyber-attacks. The results of these analyses may indicate that more complex access control is required, such as a combination of knowledge (e.g., password), property (e.g., key, smart-card) or personal features (e.g., fingerprints), rather than just a password.

[

] Based on the review of the HFC vulnerability assessments and the design conventions and platform features employed to mitigate security risk, the NRC staff determined that the design access control approach for the HFC-6000 platform has met the criterion for regulatory position 2.3.1 of RG 1.152.

3.6.3.3 Design Phase Development Activities

The regulatory position in Section 2.3.2 of RG 1.152, Revision 2, states, "The developer should delineate the standards and procedures that will conform with the applicable security policies to ensure the system design products (hardware and software) do not contain undocumented code (e.g., back door coding), malicious code (e.g., intrusions, viruses, worms, Trojan horses, or bomb codes), and other unwanted or undocumented functions or applications." [

] the NRC staff finds that the HFC-6000 platform meets the provisions of Section 2.3.2 of RG 1.152, Revision 2.

3.6.4 Implementation Phase

According to regulatory position 2.4 of RG 1.152, the implementation phase consists of the transformation of the system design into code, database structures, and related machine executable representations.

3.6.4.1 System Features

The system is indicated as consisting of integrated hardware and software. The position further identifies the scope of implementation activities as addressing hardware configuration and setup, software coding and testing, and communication configuration and setup. It is noted that the implementation activities also include the incorporation of reused software and COTS products. In addition, regulatory position 2.4.1 states that the developer should ensure that the transformation of security design configuration items from the system design specification is correct, accurate, and complete.

[

The NRC staff has reviewed the security design configuration and access control items identified above. In addition, the NRC staff traced several security features through the design and testing documentation during the two regulatory audits at the HFC facility (References 15 and 16). [

]

In performing the thread audits of security capabilities, the NRC staff found that [

]

The NRC staff finds that the implemented platform is consistent with features identified by the HFC security concept, the requirements derived from the HFC security risk assessments, and the security design items specified for the HFC-6000 platform. Consequently, the NRC staff concludes that the HFC-6000 platform has features that comply with this criterion of regulatory position 2.4.1 of RG 1.152.

3.6.4.2 Implementation Phase Development Activities

The regulatory position in Section 2.4.2 of RG 1.152, Revision 2, states, "The developer should implement security procedures and standards to minimize and mitigate tampering with the developed system. The developer's standards and procedures should include testing with scanning as appropriate, to address undocumented codes or functions that might (1) allow unauthorized access or use of the system or (2) cause systems to behave beyond the system requirements. The developer should account for hidden functions and vulnerable features embedded in the code, and their purpose and impact on the safety system. If possible, these functions should be disabled, removed, or (as a minimum) addressed to prevent any unauthorized access."

As was stated in Section 3.6.1.2 of this SE, HFC identified several vulnerabilities to the implementation phase of the platform system development:

[

]

These controls and processes are used to minimize and mitigate tampering with the developed HFC-6000 platform. In October and December of 2009, the NRC staff visited the HFC facility for regulatory audits (References 15 and 16) and was able to confirm through observation and thread audits that the cited security provisions are in place to protect the HFC-6000 platform software and assure a secure software development environment.

As noted above, development tools for the operating software of the HFC-6000 platform are also maintained in configuration controlled. The validity of these tools has been confirmed by significant usage histories and comparison of derived against previously generated code. The tools are available on development workstations in the access controlled HFC facility and operate on authorized working copies of code that are checked out from the secure repository. The development tools, including those that facilitate management of the software, are addressed in Section 3.1.3.4 of this SE.

[

]

Based upon the documented HFC efforts to fully inspect their source code for unwanted code and features, as well as the controls currently in place to protect the development environment and developed software products, the NRC staff finds that HFC complies with Section 2.4.2 of RG 1.152, Revision 2.

3.6.5 Test Phase

Regulatory position 2.5 of RG 1.152 states that the objective of testing security functions is to ensure that the security functional performance requirements are validated by execution of integration, functional, and acceptance tests where practical and necessary. This testing should include system hardware configuration (including all external connectivity) check out testing, application software object testing, software integration testing, software qualification testing, system integration testing, system qualification testing, and system factory acceptance testing.

3.6.5.1 System Features

Furthermore, regulatory position 2.5.1 of RG 1.152 states that security requirements and configuration items are to be treated as part of validation of the overall system requirements and design configuration items. Therefore, security design configuration items are just one element of the overall system validation. Each system security feature should be validated to demonstrate that the implemented system does not increase the risk of security vulnerabilities nor reduce the reliability of safety functions.

[

] Based on the cited reviews of the testing and inspection applied during the dedication of PDS and qualification of the HFC-6000 platform, the NRC staff concludes that this criterion of regulatory position 2.5.1 of RG 1.152 has been met.

3.6.5.2 Test Phase Development Activities

Regulatory position 2.5.2 of RG 1.152, Revision 2, specifies, "The developer should configure and enable the designed security features correctly. The developer should also test the system hardware architecture, external communication devices, and configurations for unauthorized pathways and system integrity. Attention should be focused on built-in OEM [original equipment manufacturer] features."

As discussed in Section 3.6.1.2 of this SE, HFC identified several vulnerabilities to the testing phase of the TXS platform system development. [

] The NRC staff concludes that HFC meets the criteria of section 2.5.2 of RG 1.152, Revision 2.

3.7 Diversity and Defense-In-Depth

The regulation at 10 CFR 50.55a(h), "Protection and safety systems," requires compliance with IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995. The regulation at 10 CFR 50.62, "Requirements for reduction of risk from anticipated transients without scram (ATWS) events for light-water-cooled nuclear power plants," requires in part various diverse methods of responding to ATWS. 10 CFR Part 50, Appendix A, 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;" and GDC 24, "Separation of protection and control systems," requires in part that "interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired."

The Staff Requirements Memorandum on SECY 93-087, dated July 21, 1993, describes the NRC position on D3 requirements to compensate for potential common-cause programming failure. This requires that the applicant assess the defense-in-depth and diversity of the proposed instrumentation and control system, and if a postulated CCF could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same CCF, shall be required to perform either the same function or a different function.

Guidance on the evaluation of diversity and defense-in-depth (D3) is provided in SRP BTP 7-19. In addition, NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," dated December 31, 1994, summarizes several D3 analyses performed after 1990 and presents a method for performing such analyses.

Additional guidance on evaluation of the need for D3, and acceptable methods for implementing the required D3 in digital I&C system designs, is contained in "Interim Staff Guidance, Digital Instrumentation and Controls, DI&C-ISG-02 Task Working Group #2: Diversity and Defense-in-Depth Issues."

Diversity and defense-in-depth is a strategy that is applied to the overall I&C system architecture in the context of a specific plant design. Section 8.6 of the TR describes a prospective plant-specific analysis approach that is derived from NUREG/CR 6303. The key assumption in this analysis is that all systems utilizing the HFC-6000 software-based platform will be subject to a software CCF and the safety functions implemented on those systems will be disabled. The NRC staff concludes that this assumption is reasonable. In the discussion of D3, HFC proposes two safety system design approaches to help address potential CCF vulnerability of the software-based platform. These approaches are separate isolated transmission of critical measurements to dedicated displays and separate implementation of critical manual actuation signals downstream of the automatic actuation output. The common feature of these design approaches is to bypass the software-based platform with transmission paths for critical measurements or actuation signals. While these are reasonable and commonly applied approaches, the effectiveness of these prospective design options in providing adequate mitigation of CCF cannot be assessed outside of the application-specific context. Thus, the performance of a plant-specific D3 analysis is an ASAI for safety-related applications of the HFC-6000 platform. The analysis determinations will be evaluated as part of a plant-specific review.

3.8 Conformance with IEEE STD 603-1991

For nuclear power generating stations, the regulation at 10 CFR 50.55a(h) requires that safety systems must meet the requirements stated in IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" and the correction sheet dated January 30, 1995. The subsections below document the evaluation of the HFC-6000 platform against those regulatory requirements. The generic SRP acceptance criteria contained in NUREG-0800, Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std 603," were used in evaluating conformance of the HFC-6000 platform with the applicable IEEE Std 603-1991 requirements. This SE supports conclusions regarding adherence of the HFC-6000 platform to the relevant regulatory requirements.

IEEE Std 603-1991 is written from a system perspective. In other words, IEEE Std 603-1991 defines criteria (i.e., contains requirements) that a safety system must meet. The evaluation documented below is performed in accordance with this system perspective. Consistent with accepted industry guidance on generic qualification of PLCs, the TR documents evidence that the PLC platform is suitable for use in safety-related applications rather than present a complete safety system design. In general, it is not possible to provide a complete assessment of conformance with system requirements on the basis of the platform alone. In the absence of a specific system design for a particular safety-related application, the determination of conformance with the IEEE Std 603-1991 requirements is necessarily limited to the evaluation of features and characteristics of the platform that support fulfillment of system requirements. Thus, the evaluation addresses the capabilities and qualifications of the platform that are relevant in assuring that a safety system based on the HFC-6000 platform satisfies regulatory requirements.

IEEE Std 603-1991 contains five clauses (Clause 4, 5, 6, 7, and 8), described in the five major subsections below, that must be considered in the evaluation of the platform. Each of these major subsections contains subordinate subsections that address the individually identifiable requirements of these clauses. Consideration is given to the degree to which each requirement can be evaluated in whole or in part within the scope of a platform review. While a number of the requirements cannot be assessed or cannot be assessed fully on the basis of the platform, each of the main requirements of IEEE Std 603-1991 is presented. This evaluation provides a means for subsequent plant-specific submittals to account for those elements of review that are contained in this document.

3.8.1 IEEE 603-1991 Clause 4, "Safety System Designation"

Clause 4 of IEEE Std 603-1991 states that a specific basis shall be established for the design of each safety system of the nuclear power generating station. The sub-clauses of this requirement can be characterized as follows:

Clause 4.1	Identification of the Design Basis Events
Clause 4.2	Safety Functions and Corresponding Protective Actions
Clause 4.3	Permissive Conditions for Each Operating Bypass Capability
Clause 4.4	Identification of Variables Monitored
Clause 4.5	Minimum Criteria for Manual Initiation And Control Of Protective Actions

Clause 4.6 Identification of the Minimum Number And Location Of Sensors
Clause 4.7 Range Of Transient and Steady State Conditions
Clause 4.8 Identification of Conditions Which May Degrade Performance
Clause 4.9 The Methods to Be Used To Determine Reliability
Clause 4.10 The Critical Points in Time After The Onset Of A Design Basis Event
Clause 4.11 The Equipment Protective Provisions
Clause 4.12 Any Other Special Design Basis

SRP Chapter 7, Appendix 7.1-C, Section 4, "Safety System Designation" provides acceptance criteria for these requirements.

The determination and documentation of the design basis for a safety system is an application-specific activity that is dependent on the plant design. Since the TR does not address a specific application of the platform, the design basis for a safety system is not available for review and no evaluation of the HFC-6000 platform against these regulatory requirements could be performed. Nevertheless, in regard to Clause 4.9, a platform-level assessment of reliability was performed by HFC and the analysis is reviewed in Section 3.8.2.15 of this SE. Of particular relevance to this requirement is the identification of the guidance of IEEE Std 352-1975 as the method used to perform the reliability determination.

3.8.2 IEEE STD 603-1991 Clause 5, "Safety System Criteria"

Clause 5 of IEEE Std 603-1991 requires that safety systems maintain plant parameters, with precision and reliability, within acceptable limits established for each design basis event. The power, instrumentation and control portions of each safety system are required to be comprised of more than one safety group of which any one safety group can accomplish the safety function.

The establishment of a safety group that can accomplish a given safety function is an application-specific activity. Since the TR does not address a specific application, the evaluation against the following regulatory requirements addresses the capabilities and characteristics of the HFC-6000 platform that are relevant for adherence to each requirement.

3.8.2.1 IEEE STD 603-1991 Clause 5.1, "Single Failure Criterion"

Clause 5.1 of IEEE Std 603-1991 requires that the safety system be able to perform its safety function 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. SRP Chapter 7, Appendix 7.1-C, Section 5.1, "Single Failure Criterion," provides acceptance criteria for the single failure criterion. In addition, RG 1.53, "Application of the Single-Failure Criterion to Safety Systems," endorses IEEE Std 379-2000, "Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," as providing an acceptable method for satisfying this requirement.

Determination that no single failure within the safety system can prevent required protective actions at the system level is an application-specific activity that requires an assessment of a full system design. A platform-level assessment can only address those features and capabilities that support adherence to the single failure criterion by a system design based on the platform. Since the TR does not address a specific application, establish a definitive safety system design, nor identify any plant I&C architectures, the evaluation against this requirement is limited to consideration of the means provided within the platform to address failures.

A FMEA is a procedure for analysis of potential failure modes within a system for determination of the effect of failures on the safety function performed by that system. The FMEA is used to address the single failure and reliability requirements of the system. This information can then be used to assess the potential for an undetectable failure or a CCF. There is no specific regulatory guidance on the required format, complexity or conclusions concerning the FMEA. The NRC staff must independently assess each to determine if the FMEA is sufficiently detailed to provide a useful assessment of potential failures and the effects of those failures.

HFC performed a FMEA for the HFC-6000 platform and documented that analysis in RR901-000-01, "Failure Modes and Effects Analysis" (Reference 141). This FMEA was performed in accordance with the provisions of Section 6.4.1 of EPRI TR-107330 and the guidance of IEEE Std 352-1987, "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems," Sections 4.1 and 4.4. However, the FMEA did not treat CCF in an extended qualitative analysis as defined in Section 4.5 of IEEE Std 352-1987.

The HFC-6000 FMEA was performed based on a generic reference system architecture composed of one instance of the platform. The basic architecture chosen for analysis consisted of a redundant-controller HFC-6000 configured with redundant chassis-mounted power supplies and representative types of I/O modules, flat panel controllers, and serial multiplexer modules. Some of the modules addressed by the analysis are not included in the scope of the platform under review (i.e., HFC-FPC06, HFC-PCC06, ECS-B232, HFC-BP08, HFC-CSM-0N, HFC-M/A-01, and HFC-FPD-01). Consequently, the analysis results specific to these modules or the functions they support were not evaluated in this review.

The FMEA addressed failures on both the system (i.e., platform) level and the module level. The system level analysis addressed the major functionality provided by the HFC-6000 platform. The module level analysis addressed individual hardware assemblies that compose the HFC-6000 platform. The analysis at this level addressed potential effects that could be caused by the failure of an individual active hardware component. Particular focus was given to failures resulting from a random bit error in RAM, PROM, or Flash memory.

HFC performed a systematic analysis of the platform to identify all credible failures, evaluate the effects of those failures on the generic representative system, determine a means of detection, and identify a means of remediation. Of the 232 postulated failure modes addressed in the analysis, only 14 were identified that could not be detected during runtime. These failure modes relate to configuration options for the HFC-6000 platform that are used only during power up initialization. Thus, these failures, which are addressed by power up diagnostics, are only evident when the controller is reset. All of the other postulated failure modes were found to result in diagnostic alarms, distinctive disruptions, and status indications that can be identified by operator surveillance. The use of redundancy generally enables the HFC-6000 platform to mitigate the effects of postulated single failures without total loss of function. However, the effects of CCF were not addressed in this FMEA. Certain failures, such as I/O module failure, can result in loss of specific functions but these failures are detectable by diagnostics or surveillance. Failures that can be detected only by surveillance (e.g., observation of anomalous behavior) were identified. However, no specific surveillance testing or monitoring procedures were recommended to address those platform-level failures for which automatic detection is not provided by self-tests or diagnostics. An application-specific FMEA must establish those surveillance provisions that are necessary to detect system failures for which automatic detection is not provided.

The NRC staff reviewed the HFC-6000 FMEA and determined that the analysis provides a useful assessment of the potential failure modes and the effect of those failures based on a generic reference system composed of one instance of the platform. The FMEA concludes that there are no undetectable single failures of the platform based on the use of redundancy, diagnostics and self-tests, and periodic surveillance as means of failure detection and indication. The NRC staff finds that the FMEA supports a conclusion that the HFC-6000 platform is suitable for use in safety-related applications in a nuclear power plant. The analysis and results of the FMEA for the HFC-6000 platform can be incorporated into application-specific FMEAs for system designs based on the platform. However, specific surveillance testing or monitoring procedures should be developed to address those identified platform-level failures that are not directly covered by the diagnostics or self-test capabilities of the platform. In addition, the analysis for an application-specific FMEA would have to be extended to address the effects of CCF in order for the results to support a conclusion about defense against CCFs in a digital safety system based on the HFC-6000 platform. Therefore, it is an ASAI for an application-specific FMEA to address the effects of CCF and to identify specific surveillance provisions to detect system failures for which automatic detection through diagnostics and self-tests are not provided (see Section 5.2 of this SE).

The architecture of the HFC-6000 platform established for safety applications employs a redundant configuration of critical components. Dual redundancy is provided for power supplies, controllers, I/O channels, and communication links. Redundancy within the platform enables it to inherently withstand most single failures of a controller or communication component without disabling the capability to perform its function. Failover between redundant components is based on failure detection and response (e.g., automated transfer of primary status based on watchdog timeout). Other design features of the HFC-6000 platform that support the capability to withstand the effects of single failures relate to independence. These features include the provision of signal channel isolation (see Section 3.3.5.5 of this SE) and the insulation of the execution of safety functions from communications transaction management (see Section 3.5.1 of this SE). The remaining identifiable single failures are addressed at the platform level through detection and indication by automatic diagnostics and self tests or periodic surveillance.

The use of redundancy at the platform level supplements the conventional use of redundancy at the system level to satisfy the single failure criterion. However, platform-level redundancy cannot substitute for system-level mitigation of the effects of a single failure on a safety function nor can it resolve potential CCF vulnerabilities. Since the HFC-6000 FMEA does not address the effects of CCF, an application-specific FMEA would have to be extended in order for the results to support a conclusion about defense against CCFs in a digital safety system based on the HFC-6000 platform. The discussion of characteristics for the HFC-6000 platform that are relevant to diversity and defense-in-depth is contained in Section 3.7 of this SE.

The HFC-6000 platform provides diagnostic and self-test capabilities to detect and enable indication of hardware faults and module component failures during power up and runtime. These capabilities are described in Section 3.4.3 of this SE. These platform-level capabilities contribute to meeting Clause 5.1 by providing the means to detect most postulated component failures. It is acknowledged in the TR and the supporting FMEA that, even with the diagnostic and self-test capabilities of the HFC-6000 platform, periodic surveillance is needed to detect some postulated failures of components, such as I/O interfaces with field devices. Consequently, provisions for surveillance testing must be established as an ASAI and evaluated as part of an application-specific review (see Section 5.2 of this SE).

The evaluation of HFC-6000 platform features and characteristics, such as redundancy, diagnostics and self test, and independence, supports a determination by the NRC staff that the platform is suitable to satisfy the single failure criterion. However, a plant-specific evaluation is necessary to establish full conformance with this regulatory requirement.

3.8.2.2 IEEE STD 603-1991 Clause 5.2, "Completion Of Protective Action"

Clause 5.2 of IEEE Std 603-1991 states that 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, and that deliberate operator action shall be required to return the safety systems to normal. SRP Chapter 7, Appendix 7.1-C, Section 5.2, "Completion of Protective Action," provides acceptance criteria for this requirement.

Determination that protective actions of the execute features of a safety system will continue to completion after initiation is an application-specific activity that requires an assessment of a full system design. Since the TR does not address a specific application and the scope of the platform does not include execute features for a safety system, no evaluation of the HFC-6000 platform against this regulatory requirement could be performed.

3.8.2.3 IEEE STD 603-1991 Clause 5.3, "Quality"

Clause 5.3 of IEEE Std 603-1991 states that the components and modules within the safety system must 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 QA program. SRP Chapter 7, Appendix 7.1-C, Section 5.3, "Quality," provides acceptance criteria for the quality requirement. This acceptance criteria states that the QA provisions of 10 CFR Part 50, Appendix B, apply to a safety system.

GDC 1 states that structures, systems, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. Where generally recognized codes and standards are used, they shall be identified and evaluated to determine their applicability, adequacy, and sufficiency and shall be supplemented or modified as necessary to assure a quality product in keeping with the required safety function. A QA program shall be established and implemented in order to provide adequate assurance that these structures, systems, and components will satisfactorily perform their safety functions. Appropriate records of the design, fabrication, erection, and testing of structures, systems, and components important to safety shall be maintained by or under the control of the nuclear power unit licensee throughout the life of the unit.

The regulation at 10 CFR 50.55a(a)(1), "Quality Standards," requires that the "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."

The HFC-6000 product line is based on a foundation of products that were designed for commercial grade industrial systems, rather than specifically for use in safety-related systems in nuclear power plants. As a result, the design process that led to the HFC-6000 platform was not governed by Appendix B of 10 CFR Part 50. The HFC-6000 platform has undergone commercial grade dedication of its system software and been subjected to Class 1E equipment qualification (see Sections 3.2.1 and 3.3, respectively, of this SE). The platform is now maintained under a software QA program intended to satisfy the requirements of Appendix B in all aspects of the product life cycle going forward with the treatment of the HFC-6000 platform (see Section 3.2.2 of this SE), including the design control process, purchasing, fabricating, handling, shipping, storing, building, inspecting, testing, operating, maintaining, repairing, and modifying of the platform.

HFC has been previously audited by an international utility member of the NUPIC. Korea Hydro and Nuclear Power Company (KHNP) conducted QA audits on four occasions in 2002 and 2007. Representatives of the KINS participated in three of those audits. As a consequence of the most recent audits, HFC is a qualified supplier of Class 1E nuclear safety systems for KHNP (Reference 14).

Application software and its specific life cycle processes are outside the scope of this review and will be treated in plant-specific reviews. The operating software for the HFC-6000 platform has undergone CGD as PDS. Based on the review of the associated development history, operating experience, life cycle design output documentation, and testing and review activities, the NRC staff finds the dedication evidence for the PDS of the HFC-6000 platform to be acceptable for demonstrating built-in quality (see Sections 3.2.1 and 3.2.3 of this SE). In addition, the NRC staff determined that the HFC QA processes for software maintenance provide reasonable confidence that the quality characteristics of the PDS can be preserved (see Section 3.2.2 of this SE). Consequently, the NRC staff concluded that the HFC-6000 hardware and operating software shows sufficient quality to be suitable for use in safety-related applications.

3.8.2.4 IEEE STD 603-1991 Clause 5.4, "Equipment Qualification"

Clause 5.4 of IEEE Std 603-1991 states that safety system equipment 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 the performance requirements as specified in the design basis. SRP Chapter 7, Appendix 7.1-C, Section 5.4, "Equipment Qualification" provides acceptance criteria for IEEE Std 603-1991 Clause 5.4. This acceptance criteria states that the applicant/licensee should confirm that the safety system equipment is designed to meet the functional performance requirements over the range of normal environmental conditions for the area in which it is located. This clause of IEEE Std 603-1991 also states that qualification of Class 1E equipment be in accordance with the requirements of IEEE Std 323-1983 and IEEE Std 627-1980, "IEEE Standard for Design Qualification of Safety Systems Equipment Used in Nuclear Power Generating Stations." RG 1.89 endorses and provides guidance on compliance with IEEE Std 323-1974 for qualification of safety-related electrical equipment installed in harsh environment locations (i.e., locations subject to design-basis-accident conditions). RG 1.209 endorses and provides guidance for compliance with IEEE Std 323-2003 for qualification of safety-related computer-based I&C systems installed in mild environment locations.

EPRI TR-107330, as accepted by an NRC SE, presents a specification in the form of a set of requirements to be applied to the generic qualification of PLCs for application and modification to safety-related I&C systems in nuclear power plants. It is intended to provide a qualification envelope corresponding to a mild environment that should meet regulatory acceptance criteria for a wide range of plant-specific safety-related applications. The qualification envelope that is established by compliance with the guidance of EPRI TR-107330 consists of the maximum (i.e., extremes) environmental and service conditions for which qualification was validated and the range of performance characteristics for the PLC that were demonstrated under exposure to environmental stress conditions. Subsequent plant-specific applications are obligated to verify that the qualification envelope provided by qualification to the guidance of EPRI TR-107330 bounds the requirements of the application.

The environmental qualification program for the HFC-6000 platform addressed the generic qualification envelope that is specified in EPRI TR-107330. The evaluation of the environmental qualification that was demonstrated is contained in Section 3.3 of this SE. Based on that evaluation, the NRC staff determined that an acceptable qualification envelope for the HFC-6000 platform was demonstrated for radiation, power surge, electrostatic discharge, and seismic withstand capabilities. In addition, the NRC staff concludes that EMC qualification of the HFC-6000 platform for radiated magnetic field, low frequency conducted interference, and high frequency conducted interference emissions has been demonstrated. Furthermore, the NRC staff finds that the HFC-6000 platform has also been demonstrated to provide acceptable isolation among signal channels and I/O modules within a safety-related system. It remains as an ASAI to verify that the generic qualification envelope for the HFC-6000 platform bounds the corresponding plant-specific conditions for these environmental stressors and that the performance characteristics demonstrated for the HFC-6000 platform under the tested service conditions are adequate for the specific application (see Section 5.2 of this SE).

The NRC staff concluded that qualification of the HFC-6000 platform has not been adequately demonstrated to establish an environmental stress withstand capability (i.e., qualification for temperature and humidity). Also, the NRC staff finds that EMC qualification of the HFC-6000 platform has not been adequately established for radiated and conducted susceptibility or for radiated electric field emissions. Demonstration of qualification against environmental stress and EMI/RFI constitutes a generic open item (see Section 5.1 of this SE). HFC has committed to conducting a retest of both environmental stress withstand capability and EMI/RFI immunity of the HFC-6000 platform (Reference 106). Until the qualification retest results or other comparable evidence are submitted for review, full environmental qualification for the HFC-6000 platform remains a generic open item.

3.8.2.5 IEEE STD 603-1991 Clause 5.5, "System Integrity"

Clause 5.5 of IEEE Std 603-1991 states that the safety systems be designed such that the system can accomplish its safety functions under the full range of applicable conditions enumerated in the design basis. SRP Chapter 7, Appendix 7.1-C, Section 5.5, "System Integrity," provides acceptance criteria for system integrity. This guidance on acceptance criteria states that the NRC staff should confirm that tests have been conducted on safety system equipment components and the system racks and panels as a whole to demonstrate that the safety system performance is adequate to ensure completion of protective actions over the range of transient and steady state conditions of both the energy supply and the environment. Furthermore, the NRC staff should confirm that tests show if the system does fail, it fails in a safe state. Also, the NRC staff should verify that failures detected by self diagnostics also place a protective function into a safe state. Finally, confirmation that system real-time performance is adequate to ensure completion of protective action within critical time frames is identified as a special concern for digital computer-based systems.

Determination of system integrity is an application-specific activity that requires an assessment of a full system design. A platform-level assessment can only address those characteristics that can support fulfillment of this requirement by a system design based on the platform. Since the TR does not address a specific application or establish a definitive safety system design, the evaluation against this requirement is limited to consideration of the integrity demonstrated by the platform and its features to assure a safe state can be achieved in the presence of failures. While the evaluation indicates the suitability of the platform to contribute to satisfying this requirement, a plant-specific evaluation is necessary to establish full conformance with Clause 5.5.

As discussed above and in Section 3.3 of this SE, the HFC-6000 platform underwent testing to demonstrate qualification for installation in mild environment locations in a nuclear power plant. Pending satisfactory resolution of the generic open items regarding environmental qualification as captured in Section 5.1 of this SE, the HFC qualification program provides reasonable assurance that safety-related systems based on the HFC-6000 platform will be capable of performing safety functions over the full range of environmental conditions that correspond to those expected worst case design basis events bounded by the qualification envelope for the HFC-6000 platform. Based on review of the environmental qualification evidence, the HFC-6000 platform currently partly satisfies the acceptance criteria for those environmental conditions that have been demonstrated under the HFC qualification program.

The NRC staff review of the FMEA for the HFC-6000 platform is discussed in Section 3.8.2.1 of this SE. The FMEA was based on a generic reference system architecture and provides reasonable assurance that platform failures, including loss of power failures, can be accommodated by the redundancy features of the platform, detected and alarmed (i.e., included in status information that can be transmitted for display) by the diagnostics and self-test capabilities of the platform, or identified through periodic surveillance and operator monitoring at the system level. The redundancy provided by the HFC-6000 platform provides automatic failover for disabling failures of a single redundant feature and alarms the condition through status information that is displayed locally (i.e., board-edge LEDs) and can be transmitted for display. The NRC staff finds that the redundancy features of the HFC-6000 platform provide fault tolerance and allow a safe state to be maintained through continued operation for a large number of identified failures. The diagnostics and self-test capabilities of the HFC-6000 platform, which are discussed in Section 3.4.3 of this SE, provide acceptable means for placing the system in a safe state and alarming the failure condition for those failures detected by diagnostics. In many instances, the safe state can consist of a failover from primary to secondary controller. However, the specific response to particular failures depends on an application-specific system design and is, therefore, subject to a plant-specific review.

The platform-level FMEA does not address the means for annunciating failures since HMIs are not within the scope of the base platform and, thus, cannot be evaluated in this review. Also, the provision of surveillance testing and operator monitoring of those identified failures that are not automatically detected by diagnostics or self-test depends on an application-specific system design, which can include application-level diagnostics and status indication to operators. Consequently, it is an ASAI for an application-specific FMEA to identify specific surveillance provisions to detect system failures for which automatic detection through diagnostics and self-tests are not provided (see Section 5.2 of this SE).

The output modules of the HFC-6000 provide selectable preferred states or seal-in circuitry for loss of power or reset conditions, as described in Sections 3.1.1.6.2, 3.1.1.6.3, 3.1.1.6.4, and 3.1.1.6.7 of this SE. These capabilities were demonstrated through loss of power testing under the HFC qualification program (References 92, 123, and 124). Although determination of a safe state is application and plant specific, the capability to enter a predefined safe state upon loss of power or failure detection is provided by the HFC-6000 platform. Thus, based on review of the FMEA, qualification results, diagnostics, and platform design features, the NRC staff has determined that the HFC-6000 provides capabilities and features (e.g., redundancy, diagnostics, and failsafe output configurability) that provide a suitable basis for satisfying this portion of the acceptance criteria.

The evaluation of response time and deterministic performance is discussed in Sections 3.4.1 and 3.4.2 of this SE. Although the HFC-6000 platform did not satisfy the response time criteria from EPRI TR-107330 for the test specimen executing the synthetic TSAP application, the platform did demonstrate credible response time characteristics that are suitable to support safety-related applications. The actual response times for particular safety functions are application specific and acceptable performance depends on the system design and safety function requirements. Thus, it is an ASAI to confirm the suitability of the response time characteristics of the HFC-6000 platform for particular safety functions and to demonstrate acceptable response times for each combination of input and output modules that are relevant to the specific design (see Section 5.2 of this SE). Consequently, evaluation for full conformance against this portion of the acceptance criteria remains for a plant-specific review.

Based on the review items discussed above, the NRC staff finds that the integrity characteristics (e.g., response time, deterministic performance, failure detection and response, fault tolerance, environmental withstand) of the HFC-6000 platform, when appropriately implemented, are suitable for safety-related applications at nuclear power plants.

3.8.2.6 IEEE STD 603-1991 Clause 5.6, "Independence"

Clause 5.6 of IEEE Std 603-1991 requires in part 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 system integrity. This acceptance criteria states that three aspects of independence: (1) physical independence, (2) electrical independence, and (3) communications independence, should be addressed for each of the previously listed cases. 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 Std 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 should include the utilization of separate power sources. Transmission of signals between independent channels should be through isolation devices.

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 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 nonsafety system, a logical or software malfunction of the nonsafety system must not be able to affect the functions of the safety system.

Establishing independence for a safety system is an application-specific activity that requires an assessment of a full system design. A platform-level assessment can only address those capabilities and qualifications that can support adherence to the independence requirement by a system design based on the platform. Since the TR does not address a specific application or establish a definitive safety system design, the evaluation against this requirement is limited to consideration of the means provided within the platform to promote independence. Of the three types of independence identified for this requirement (i.e., physical, electrical, and communications), the HFC-6000 platform provides features to address electrical and communications independence. Physical independence is solely dependent on the design and implementation of the full safety system.

Two means of digital communication are provided by the HFC-6000 platform: the C-Link network for broadcast of status data and the ICL serial bus for communication between the controller modules and I/O modules. The C-Link involves broadcast communication among safety nodes (i.e., instances of the HFC-6000 platform) across an internal network (i.e., intra-channel communication). The ICL serves as the communication path for input and output data. Electrical independence of each communication link involves electro-optical means to isolate the communication interconnections electrically.

The C-Link is designed to support use of electro-optical converters and fiber optic cable. However, the ECS-B232 fiber optic transmitters and the transmission medium (i.e., wires or fibers) intended for use in the C-Link network are not included in the scope of the base platform. The restriction in scope of the HFC-6000 platform precludes a platform level evaluation of electrical independence for any uses of the C-Link to interconnect with redundant portions of a safety system or with other systems (e.g., safety to nonsafety). In those cases, provision of electrical isolation for C-Link interconnections with external devices is an ASAI that can be evaluated as part of a plant-specific review (see Section 5.2 of this SE).

The HFC-6000 detailed design descriptions for the I/O modules (References 35 through 42) describe the electrical isolation features for analog and digital inputs and outputs connected to the ICL bus. [

] The environmental qualification of the HFC-6000 platform (see Section 3.3 of this SE) included isolation testing to demonstrate the capability to satisfy the Class 1E to non-Class 1E isolation provisions specified in EPRI TR-107330, which are consistent with the provisions of IEEE Std 384-1992. The isolation tests demonstrated adequate capability of the I/O modules to support Class 1E to non-Class 1E isolation. On the basis of the electrical isolation testing, the NRC staff concludes that the isolation provided by the analog and digital I/O modules connected by the ICL is suitable for use in satisfying the electrical independence requirement of Clause 5.6.

Section 3.5.1 of this SE discusses the use of interposing processors to buffer the execution of the safety function by the SYS processor from the management of communications transactions by the C-Link and ICL subordinate processors. Section 3.5.2 of this SE addresses the evaluation of communications independence with respect to the guidance in DI&C-ISG-04. Sections 3.8.2.6.3.1 and 3.9.1.4 of this SE address communications independence in terms of system dependencies. Section 3.6.3.2 of this SE discusses communications independence in terms of security design access control. The platform communication capabilities of the HFC-6000 platform provide features that can support communications independence but the specific interconnections defined in an application must be determined and evaluated in an application-specific review.

Thus, the review items cited above indicate provisions for electrical isolation and communications circuitry and protocols to promote communications independence. Consequently, the NRC staff concludes that the HFC-6000 platform complies with the electrical and communications provisions of this clause at the platform level.

Nevertheless, a plant-specific evaluation is necessary to establish full conformance with Clause 5.6.

3.8.2.6.1 IEEE STD 603-1991 Clause 5.6.1, "Between Redundant Portions of a Safety System"

Clause 5.6.1 of IEEE Std 603-1991 states that the safety systems be designed such that there is sufficient independence between redundant portions of a safety system such that the redundant portions are 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. SRP Chapter 7, Appendix 7.1-C does not provide any additional acceptance criteria beyond that in Clause 5.6.1.

The redundant configuration of a multi-channel safety system and the independence provided between those redundant channels are solely dependent on the safety system design. The base architecture presented for the HFC-6000 platform is representative of a single channel in a safety system. Since the TR does not address a specific application or establish a definitive safety system design, no evaluation of the HFC-6000 platform against this regulatory requirement could be performed.

3.8.2.6.2 IEEE STD 603-1991 Clause 5.6.2, "Between Safety Systems and Effects of Design Basis Event"

Clause 5.6.2 of IEEE Std 603-1991 states that the safety systems required to mitigate the consequences of a specific design basis event must 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. Clause 5.6.2 further states that equipment qualification in accordance with 5.4 is one method that can be used to meet this requirement.

The regulation at 10 CFR Part 50, Appendix A, GDC 22, "Protection system independence," requires in part that the protection system be designed to assure that the effects of natural phenomena and of normal operating, maintenance and testing do not result in loss of protection function.

Determining the effects of design basis events and establishing the physical separation of the safety system from the effects of those events are application-specific activities. However, the qualification of the HFC-6000 platform under the generic service conditions required in EPRI TR-107330 can be used to demonstrate the capability of a safety system based on the platform to satisfy this requirement. The evaluation of the environmental qualification for the HFC-6000 platform is contained in Sections 3.3 and 3.8.2.4 of this SE. As is the case for fulfilling the requirement of IEEE Std 603-1991, Clause 5.4, it remains as an ASAI to verify that the generic qualification established for the HFC-6000 platform bounds the plant-specific conditions (i.e., temperature, humidity, seismic, and electromagnetic compatibility) for the locations(s) in which the HFC-6000 equipment is to be installed and that the performance characteristics of the HFC-6000 platform demonstrated under the tested service conditions are adequate for the specific application (see Section 5.2 of this SE).

3.8.2.6.3 IEEE STD 603-1991 Clause 5.6.3, "Between Safety Systems and Other Systems"

Clause 5.6.3 of IEEE Std 603-1991 states that the safety systems be designed such that credible failures in and consequential actions by other systems will not prevent the safety systems from meeting the requirements of this standard. This requirement is subdivided into requirements for interconnected equipment, equipment in proximity, and the effects of a single random failure. SRP Chapter 7, Appendix 7.1-C does not provide any additional acceptance criteria beyond that in Clause 5.6.3.

The three subsections below document the evaluation of interconnected equipment, equipment in proximity, and the effects of a single random failure separately.

3.8.2.6.3.1 IEEE STD 603-1991 Clause 5.6.3.1, "Interconnected Equipment"

Clause 5.6.3.1 of IEEE Std 603-1991, "Interconnected Equipment," states that equipment that is used for both safety and nonsafety functions, as well as the isolation devices used to affect a safety system boundary, be classified as part of the safety systems. This clause further states that no credible failure on the nonsafety 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, and that a failure in an isolation device will be evaluated in the same manner as a failure of other equipment in a safety system.

Determination of interconnections between a safety system and other nonsafety systems in a plant through common equipment or communication links is an application-specific activity. The base platform architecture identified in the TR does not specify any direct connections or bi-directional communication between the HFC-6000 and any other system. However, the TR does identify the capability for one-way communication to nonsafety-related components across the C-Link network though fiber optic cabling and an isolation gateway. To promote independence, HFC established a design principle for nuclear safety applications that restricts communication over the C-Link network to broadcast-only messages so peer-to-peer communication is not allowed (Reference 21). However, the gateway and network medium are not part of the base platform and, thus, are not within the scope of this evaluation. Consequently, fulfilling this requirement involves an ASAI for verification that the gateway (or any other device not part of the base HFC-6000 platform) cannot transmit messages on the C-Link and thus compromise independence between the safety system and any other systems connected to the gateway (see Section 5.2 of this SE).

3.8.2.6.3.2 IEEE STD 603-1991 Clause 5.6.3.2, "Equipment in Proximity"

Clause 5.6.3.2 of IEEE Std 603-1991, "Equipment in Proximity," states that 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, will 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 nonsafety equipment, and that physical separation may be achieved by physical barriers or acceptable separation distance. This clause states that the separation of Class 1E equipment shall be in accordance with the requirements of IEEE Std 384-1981. This clause further states that the physical barriers used to establish a safety system boundary shall meet the requirements of 5.3, "Quality," 5.4, "Equipment Qualification" and 5.5, "System Integrity" for the applicable conditions specified in 4.7 and 4.8 of the design basis.

Determination of the physical proximity of safety system equipment in relation to other equipment in a plant is an application-specific activity. Since the TR does not address a specific application or specify plant locations for implementation, no evaluation of the HFC-6000 platform against this regulatory requirement could be performed.

3.8.2.6.3.3 IEEE STD 603-1991 Clause 5.6.3.3, "Effects of a Single Random Failure"

Clause 5.6.3.3 of IEEE Std 603-1991, "Effects of a Single Random Failure," states that where a single random failure in a nonsafety 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.

Determination of potential failure propagation paths through interconnections between a safety system and other nonsafety systems in a plant is generally an application-specific activity. The base platform architecture identified in the TR does not specify any direct connections or bi-directional communication between the HFC-6000 and any other system. Since the TR does not address a specific application or specify interconnections with other systems, no evaluation of the HFC-6000 platform against this regulatory requirement could be performed.

3.8.2.6.4 IEEE STD 603-1991 Clause 5.6.4, "Detailed Criteria"

This clause does not contain any requirements; therefore no evaluation against this part is required.

3.8.2.7 IEEE STD 603-1991 Clause 5.7, "Capability for Test and Calibration"

Clause 5.7 of IEEE Std 603-1991 states that the safety system shall have the capability for test and calibration while retaining the capability to accomplish its safety function, and that this capability be provided during power operation and shall duplicate, as closely as practicable, performance of the safety function. This clause further states that the testing of Class 1E systems be in accordance with the requirements of IEEE Std 338-1987. Exceptions to testing and calibration during power operation are allowed where this capability cannot be provided without adversely affecting the safety or operability of the generating station; however, appropriate justification must be provided; acceptable reliability of equipment operation must demonstrated; and the capability shall be provided while the generating station is shut down.

SRP Chapter 7, Appendix 7.1-C, Section 5.7, "Capability for Test and Calibration," provides acceptance criteria for IEEE Std 603-1991 Clause 5.7. First, it states that guidance on periodic testing of the safety system is provided in RG 1.22, "Periodic Testing of Protection System Actuation Functions," and in RG 1.118, Revision 3, "Periodic Testing of Electric Power and Protection Systems," that endorses IEEE Std 338-1987. Section 5.7 acceptance criteria states that periodic testing should duplicate, as closely as practical, the overall performance required of the safety system, and that the test should confirm operability of both the automatic and manual circuitry. This capability should be provided to permit testing during power operation and that when this capability can only be achieved by overlapping tests, the test scheme must be such that the tests do, in fact, overlap from one test segment to another. Section 5.7 further states that test procedures that require disconnecting wires, installing jumpers, or other similar modifications of the installed equipment are not acceptable test procedures for use during power operation. Section 5.7 further states that for digital computer based systems, test provisions should address the increased potential for subtle system failures such as data errors and computer lockup.

The regulation at 10 CFR Part 50, Appendix A, GDC 21, "Protection system reliability and testability," requires in part that the protection system be designed for in-service testability commensurate with the safety functions to be performed. It also requires a design that permits periodic testing of its functioning when the reactor is in operation, including the capability to test channels independently to determine failures and losses of redundancy that may have occurred.

The regulation at 10 CFR 50.36(c)(3), "Technical Specifications," states that surveillance requirements are requirements relating to test, calibration, or inspection to assure that the necessary quality of systems and components is maintained, that facility operation will be within safety limits, and that the limiting conditions for operation will be met.

RG 1.53, "Application of the Single-Failure Criterion to Safety Systems," which endorses IEEE Std 379-2000, "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," states that the protection system must be capable of accomplishing the required protective function in the presence of any single detectable failure concurrent with all identifiable, but non-detectable, failures. Consequently, self-testing and periodic testing are important elements in the design's ability to meet the single-failure criterion.

SRP BTP 7-17 describes additional considerations in the evaluation of test provisions in digital computer based systems.

Determination of the test and calibration requirements that must be fulfilled depends upon the plant-specific safety requirements (e.g., accuracy) that apply. In addition, the establishment of the types of surveillance necessary for the safety system to ensure detection of identifiable single failures that are only announced through testing is an application-specific activity. Since the TR does not address a specific application or establish a definitive safety system design, the evaluation against this requirement is limited to consideration of the means provided within the platform to enable testing and calibration for a redundant portion of a safety system (i.e., channel).

The HFC FMEA (see Section 3.8.2.1 of this SE) provided a systematic analysis of a representative (single-channel) system based on the HFC-6000 platform to determine the effect on the system (i.e., platform) of credible single failures. For each postulated failure mode, the FMEA determined ways in which the failure could be detected. Failures that can be detected only by surveillance were clearly identified. However, no specific recommendations on testing to detect any particular failures were provided. In addition, the TR does not specify periodic surveillance testing or define surveillance intervals (see Section 3.8.2.15 of this SE). These provisions must be established as an ASAI and evaluated as part of an application-specific review to allow the capability for test and calibration to be fully determined (see Section 5.2 of this SE).

Diagnostics and self-test capabilities of the HFC-6000 platform are described in Section 3.4.3 of this SE. These software functions are thorough and provide automatic detection of most identified failure modes at the platform level. The TR describes acceptable use of software watchdog timers, memory checks, processing time checks, communications checks, loop back tests and other tests in each type of component as appropriate to verify normal operation.

Automatic calibration tests for the AI16F and AI8M modules provide detection of operability and correction for drift. Every scan cycle, the analog input module reads precision internal reference voltages and automatically calibrates the input. The self-diagnostics can detect drift in the input circuit or reference power supply. When the drift is outside the acceptable limits, the module sets an indicator corresponding to a calibration error alarm. These self-calibrate features do not calibrate the entire instrument string—just the ADC processing. It is acknowledged that tests of components not part of the platform itself would have to be covered by manual tests.

Validation of software in memory by checksum calculation is another type of automated test provided by the HFC-6000 platform. This capability during initialization and runtime provides an automatic check to ensure that software has not been changed or corrupted. In addition, the checksum of the application software is validated at the start of each execution cycle.

The diagnostic and self-test features, including automatic calibration, contribute to satisfying this requirement for test and calibration capabilities and are, therefore, acceptable. These capabilities may be cited in support of specific applications. However, as noted in the discussion of the FMEA findings (see Section 3.8.2.1 of this SE), the software diagnostics and self-tests do not provide comprehensive automatic coverage of all platform failures nor are they sufficient in and of themselves to eliminate the need for periodic surveillance testing (i.e., the HFC FMEA identifies some failures that require surveillance for detection). Consequently, it is an ASAI is to establish what additional surveillance is necessary to ensure that the identifiable failure modes of the safety system are acceptably covered by the available testing and calibration capabilities (See Section 5.2 of this SE), as well as any applicable alarm display mechanisms.

It is established in the TR and supplemental documentation (References 47, 48, 49, and 141) that the HFC-6000 platform provides the capability for test and some degree of calibration checking in conjunction with the online, real-time execution of its safety function. In effect, the HFC-6000 software architecture is designed to provide for automatic tests and diagnostics to be performed as part of the execution sequence within each context switch interval. These test and calibration capabilities are acceptable for meeting this regulatory requirement at the platform level. However, since system-level testing (e.g., automated function tests embedded within the application code and manual surveillance tests) and HMIs for initiating and conducting such tests are not within the scope of the TR, full satisfaction of this requirement is application specific. Therefore, while the evaluation confirms the suitability of the platform to contribute to satisfying this requirement, a plant-specific evaluation is necessary to establish full conformance with Clause 5.7.

3.8.2.8 IEEE STD 603-1991 Clause 5.8, "Information Displays"

Clause 5.8 of IEEE Std 603-1991 has four sub-clauses, 5.8.1, "Displays for Manually Controlled Actions," 5.8.2, "System Status Indication," 5.8.3, "Indication of Bypasses," and 5.8.4, "Location." Appendix 7.1-C, Section 5.8, "Information Displays," provides acceptance criteria for IEEE 603, Clause 5.8. This guidance states that the information displays for manually controlled actions should include confirmation that displays will be functional, and that safety system bypass and inoperable status indication should conform to the guidance of RG 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems."

The design of information displays and operator workstations is an application-specific activity. Since the TR does not address a specific application nor include display devices (other than local faceplate LEDs) within the scope of the platform, the evaluation against the following regulatory requirements addresses the capabilities and characteristics of the HFC-6000 platform that are relevant for adherence to each requirement.

3.8.2.8.1 IEEE STD 603-1991 Clause 5.8.1, "Displays for Manually Controlled Actions"

Clause 5.8.1 states that 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 will be part of the safety systems and will meet the requirements of IEEE Std 497-1981. The design shall minimize the possibility of ambiguous indications that could be confusing to the operator. SRP Chapter 7, Appendix 7.1-C, Section 5.8, "Information Displays," provides no further review guidance for Clause 5.8.1.

Determination of the display provision for manually controlled actions is an application-specific activity. Since the TR does not address a specific application nor include display devices within its scope, no evaluation against this regulatory requirement could be performed.

3.8.2.8.2 IEEE STD 603-1991 Clause 5.8.2, "System Status Indication"

Clause 5.8.2 states that display instrumentation must provide accurate, complete, and timely information pertinent to safety system status, and further this information shall include indication and identification of protective actions of the sense and command features and execute features. Clause 5.8.2 further states that the design minimize the possibility of ambiguous indications that could be confusing to the operator; however, the display instrumentation provided for safety system status indication need not be part of the safety systems. SRP Chapter 7, Appendix 7.1-C, Section 5.8, "Information Displays," provides no further review guidance for IEEE Std 603-1991 Clause 5.8.2. The alarm and indication systems related to the status of the overall safety system or plant equipment are dependent on the application. Thus, determination of the means for safety system status indication is an application-specific activity. Since the TR does not address a specific application nor include display devices within its scope, no evaluation against this regulatory requirement could be performed.

3.8.2.8.3 IEEE STD 603-1991 Clause 5.8.3, "Indication of Bypass"

Clause 5.8.3 states that 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. Clause 5.8.3 further states that this display instrumentation need not be part of the safety systems, that this indication shall be automatically actuated if the bypass or inoperative condition is expected to occur more frequently than once a year, and is expected to occur when the affected system is required to be operable, that the capability shall exist in the control room to manually activate this display indication, and that the 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. SRP Chapter 7, Appendix 7.1-C, Section 5.8, "Information Displays," provides no further review guidance for IEEE 603 Clause 5.8.3.

RG 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems," describes an acceptable method of complying with the requirements of IEEE Std 603-1991, Clause 5.8.3.

Bypass status of a safety division is a function of the multi-division arrangement of the application. Thus, determination of the means for bypassed or inoperable status indication is an application-specific activity. Since the TR does not address a specific application nor include display devices within its scope, no evaluation against this regulatory requirement could be performed.

3.8.2.9 IEEE STD 603-1991 Clause 5.9, "Control of Access"

Clause 5.9 of IEEE Std 603-1991 states that the safety system must be designed to permit administrative control of access to safety system equipment. SRP Chapter 7, Appendix 7.1-C, Section 5.9, "Control of Access," provides acceptance criteria for IEEE Std 601-1991 Clause 5.10. This acceptance criteria states that administrative control is acceptable to assure that the access to the means for bypassing safety system functions is limited to qualified plant personnel and that permission of the control room operator is obtained to gain access, and that digital computer based systems need to consider controls over electronic access, including access via network connections and maintenance equipment, to safety system software and data.

Establishing the particular approach for control of access to safety system equipment is an application-specific activity that depends on the system design. Physical access mechanisms depend on the specific implementation. The extent and nature of authorized human-system interactions depend on the allocation of function, operations and maintenance procedures, and human-machine interface capabilities addressed in a safety system design. In addition, the communication interconnections that may be provided between the safety system and other safety-related or nonsafety system or equipment are generally dependent on the application. Since the TR does not address a specific application, the evaluation against this requirement is limited to consideration of the means provided within the platform to control access to both hardware and software.

The HFC-6000 is a modular, rack mounted platform that is housed in cabinets. However, the cabinets themselves are not identified as part of the base platform and thus are not within the scope of this review. Consequently, the mechanisms for physical access control cannot be evaluated in this review.

Although the HFC-6000 product line includes display and peripheral component (e.g., control stations) interface modules that can support online human-system interactions across the ICL, these modules are not within the scope of the platform under review. As submitted for review, the base architecture does not contain any provision for external communication to the HFC-6000 platform across the C-Link by other devices (e.g., operator or testing/maintenance workstations). Thus, control of electronic access through provisions associated with HMIs cannot be evaluated in this review.

[

]

The HFC Engineering Workstation (EWS) serves as a maintenance workstation that supports offline, out-of-service management (e.g., development and installation) of application software. The EWS is not part of the base platform so it is not within the scope of this review. Nevertheless, it is noted that the base platform architecture described in the TR does not provide for direct or network connection of the EWS to the HFC-6000 platform for online maintenance. Any such connection that may be established in a specific application would require additional review.

The NRC staff has evaluated the HFC-6000 platform features to provide control of access and finds that they are sufficient at the platform level. While the evaluation indicates the suitability of the platform to contribute to satisfying this requirement, a plant-specific evaluation is necessary to establish full conformance with Clause 5.9.

3.8.2.10 IEEE STD 603-1991 Clause 5.10, "Repair"

Clause 5.10 of IEEE Std 603-1991 states that safety systems must be designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment. SRP Chapter 7, Appendix 7.1-C, Section 5.10, "Repair" provides acceptance criteria for IEEE Std 601-1991 Clause 5.10. This acceptance criteria states that while digital safety systems may include self diagnostic capabilities to aid in troubleshooting, the use of self diagnostics does not replace the need for the capability for test and calibration systems as required by Clauses 5.7 and 6.5 of IEEE Std 603-1991.

The timely identification and location of malfunctioning HFC-6000 components is facilitated by platform and application-specific (hardware and software) features. Any diagnostic and self-test functions developed as part of the application software (e.g., signal validation) are outside the scope of this evaluation and are treated in an application-specific review. The majority of HFC-6000 hardware is rack mounted and is replaced rather than repaired, which greatly facilitates timely repair.

The HFC-SBC06 board contains sixteen board-edge LEDs to provide a visual indication of functional status of the controller hardware and software. Eight of the LEDs are used to indicate status and activity of C-Link and ICL communication. The other eight LEDs display a binary code for the task that is executing during normal operation. If a fault occurs during runtime or initialization, these LEDs indicate a binary code for the detected fault condition to facilitate troubleshooting by indicating the error type. The HFC-DPM06 board contains five board-edge LEDs to provide a visual indication of the functional status of each redundant controller (i.e., primary or secondary role and "sanity" status) and availability of the failover function.

The redundant controllers of the HFC-6000 platform provide a maintenance failover pushbutton on the faceplate of the HFC-DPM06 module to allow failover between primary and secondary controllers to be triggered manually. This feature enables testing of the failover function and supports replacement of a controller module. It is available when both redundant controllers are "sane."

The platform software for the HFC-6000 includes diagnostic and self-test functions (see Section 3.4.3 of this SE). The HFC-6000 FMEA identifies failure modes that are automatically detected by diagnostic and self-test functions. However, the FMEA also identifies failure modes that are detectable only by surveillance (see Section 3.8.2.1 of this SE). Thus, the diagnostic and self-test functions of the HFC-6000 platform do not replace the need for test and calibration systems.

Based on the provision of automatic diagnostics and self tests to detect and identify most failures of the platform, the NRC staff evaluation finds that the HFC-6000 platform complies with this requirement. However, it is necessary for an application-specific design to provide additional diagnostics or testing functions either as part of the application or as manually-conducted testing to address those system-level failures that are identified as detectable only through periodic surveillance. Thus, a plant-specific review would be necessary to address physical configuration and plant-specific installation conditions that impact safety system maintenance or to evaluate any necessary diagnostic, testing, or surveillance functions implemented in application software.

3.8.2.11 IEEE STD 603-1991 Clause 5.11, "Identification"

Clause 5.11 of IEEE Std 603-1991 states that (1) safety system equipment shall be distinctly identified for each redundant portion of a safety system in accordance with the requirements of IEEE Std 384-1981, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits," and IEEE Std 420-1982, "IEEE Standard for the Design and Qualification of Class 1E Control Boards, Panels, and Racks Used in Nuclear Power Generating Stations," (2) identification of safety system equipment shall be distinguishable from any identifying markings placed on equipment for other purposes, (3) identification of safety system equipment and its divisional assignment shall not require frequent use of reference material, and (4) the associated documentation shall be distinctly identified in accordance with the requirements of IEEE Std 494-1974 (R1990), "IEEE Standard Method for Identification of Documents Related to Class 1E Equipment and Systems for Nuclear Power Generating Stations." Clause 5.11 further states that 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. SRP Chapter 7, Appendix 7.1-C, Section 5.11, "Identification," provides acceptance criteria for Clause 5.11 and cites the guidance in RG 1.75, "Criteria for Independence of Electric Systems," which endorses IEEE Std 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits."

Coding of cabinets and cabling for a safety system is an application-specific activity. In addition, the particular means for identifying safety equipment according to redundant portions of a safety system (i.e., channels or divisions) is an application-specific activity. However, component identification for the HFC-6000 platform can contribute to fulfillment of this requirement. The HFC QA Program defines requirements for the identification and control of items and provides procedures for establishing and maintaining system configuration management (References 80 and 90). Under its System Configuration Management Program, HFC has established labeling, tracking and record keeping practices and capabilities to control the identification of components. In addition to faceplate identification of module type, HFC provides physical labels on the printed circuit board of each module to uniquely identify the hardware module and installed firmware. As part of the regulatory audits conducted at the HFC facility (References 15 and 16), NRC staff observed component identification based on the physical labels applied to representative modules.

The NRC staff finds that the identification procedures and methods for the HFC-6000 platform complies with this regulatory requirement and are suitable to support fulfillment of this clause by a safety-related system. Identification of operating software is discussed in Section 3.9.1.8 of this SE. As noted, identification of the redundant portions of a safety system (i.e., channels or divisions) is necessarily plant specific. Any supplementary identification approach employed at the system-level will be addressed in a plant-specific review to assure satisfaction of Clause 5.11.

3.8.2.12 IEEE STD 603-1991 Clause 5.12, "Auxiliary Features"

Clause 5.12 of IEEE Std 603-1991 states that auxiliary supporting features meet all requirements of this standard, and that auxiliary features that perform a function that is not required for the safety systems to accomplish their safety functions and are 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. SRP Chapter 7, Appendix 7.1-C, Section 5.12, "Auxiliary Features," provides acceptance criteria for Clause 5.12 and cites SRP BTP 7-9, "Guidance on Requirements for Reactor Protection System Anticipatory Trips," as providing specific guidance for the review of anticipatory trips that are auxiliary features of a reactor protection system.

Determination of auxiliary supporting features for a safety system is an application-specific activity. Since the TR does not address a specific application, no evaluation of the HFC-6000 platform against this regulatory requirement could be performed.

3.8.2.13 IEEE STD 603-1991 Clause 5.13, "Multi-Unit Stations"

Clause 5.13 of IEEE Std 603-1991 states that 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, and that guidance on the sharing of electrical power systems between units is contained in IEEE Std 308-1980 "IEEE Standard Criteria for Class IE Power Systems for Nuclear Power Generating Stations," and guidance on the application of the single failure criterion to shared systems is contained in IEEE Std 379-1988, "Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems." SRP Chapter 7, Appendix 7.1-C, Section 5.13, "Multi Unit Stations," provides acceptance criteria for Clause 5.13. This acceptance criterion states that the shared user interfaces must be sufficient to support the operator needs for each of the shared units. Implementation of a safety system in a multi-unit station and determination of components can be shared is an application-specific activity. Since the TR does not address a specific application, no evaluation of the HFC-6000 platform against this regulatory requirement could be performed.

3.8.2.14 IEEE STD 603-1991 Clause 5.14, "Human Factors Considerations"

Clause 5.14 of IEEE Std 603-1991 states that human factors 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 operators and maintainers can be successfully accomplished to meet the safety system design goals. SRP Chapter 7, Appendix 7.1-C, Section 5.14, "Human Factors Considerations," provides acceptance criteria for Clause 5.14, and states that safety system human factors design should be consistent with the applicant/licensee's commitments documented in Chapter 18 of the Updated Safety Analysis Report (USAR).

Implementation of human factors considerations to address functional allocation is an application-specific activity. Since the TR does not address a specific application nor include display devices within its scope, no evaluation of the HFC-6000 platform against this regulatory requirement could be performed.

3.8.2.15 IEEE STD 603-1991 Clause 5.15, "Reliability"

Clause 5.15 of IEEE Std 603-1991 states that 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, and that IEEE Std 352-1987 and IEEE Std 577-1976 provide guidance for reliability analysis. SRP Chapter 7, Appendix 7.1-C, Section 5.15, "Reliability," provides acceptance criteria for Clause 5.15. This acceptance criterion states that the applicant/licensee should justify that the degree of redundancy, diversity, testability, and quality provided in the safety system design is adequate to achieve functional reliability commensurate with the safety functions to be performed and that for computer systems, both hardware and software reliability should be analyzed. The acceptance criteria further states that software that complies with the quality criteria of IEEE Std 603-1991 Clause 5.3 and that is used in safety systems that provide measures for defense against common cause failures, as previously described for IEEE Std 603-1991 Clause 5.1, are considered by the NRC staff to comply with the fundamental reliability requirements of GDC 21, IEEE Std 279-1971, and IEEE Std 603-1991.

SRP Chapter 7, Appendix 7.1-C, Section 5.15 further states that the assessment of reliability should consider the effect of possible hardware and software failures and the design features provided to prevent or limit the effects of these failures, and that hardware failure conditions to be considered should include failures of portions of the computer itself and failures of portions of communication systems. Hard failures, transient failures, sustained failures, and partial failures should be considered. Software failure conditions to be considered should include, as appropriate, software common cause failures, cascading failures, and undetected failures. SRP Chapter 7, Appendix 7.1-C, Section 5.15 also references SRP Chapter 7, Appendix 7.1-D, and points out that quantitative reliability goals are not sufficient as a sole means of meeting the Commission's regulations for the reliability of digital computers used in safety systems.

The regulation at 10 CFR 50, Appendix A, GDC 21, "Protection system reliability and testability," requires in part that the protection system be designed for high functional reliability commensurate with the safety functions to be performed.

Determination of the reliability of a safety system is an application-specific activity that requires an assessment of a full system design. Since the TR does not address a specific application, establish a definitive safety system design, nor identify any plant I&C architectures, the evaluation against this requirement is limited to consideration of the reliability characteristics of the platform and its components.

Based on the guidance of EPRI TR-107330, HFC performed analyses to indicate the reliability of the HFC-6000 platform. An FMEA was performed in accordance with IEEE Std 352-1987 based on a generic reference system architecture. The NRC staff's evaluation of the FMEA determined that it provides a useful assessment of the potential failure modes and the effect of those failures at the platform level. Based on the use of redundancy, diagnostics and self-tests, and periodic surveillance as means of failure detection and indication, no undetectable single failures of the HFC-6000 platform were identified in the FMEA. However, an extension of the analysis to address the effects of CCF is necessary for an application-specific FMEA to support a conclusion about defense against CCFs in a digital safety system based on the HFC-6000 platform (see Section 5.2 of this SE).

HFC performed a reliability and availability analysis of the HFC-6000 platform as specified in Section 4.2.3 of EPRI TR-107330 and documented the results in RR901-000-04, "Reliability and Availability Analysis Report" (Reference 143). Following the guidance in EPRI TR-107330, a representative system configuration, based on a single instance of the redundant-controller platform along with other peripheral interface modules that are not included in the platform scope, was used as the basis for the analysis. The analysis determined that the calculated reliability and availability of a typical system based on the HFC-6000 platform are greater than 99.94 percent, which exceeds the goal of 99.0 percent established by EPRI TR-107330.

Consistent with the guidance in EPRI TR-107330, the HFC-6000 availability calculations include only random hardware failure rates. Software CCF probabilities are excluded in EPRI TR-107330 because "there is presently no agreed upon method for establishing software failure rates...except through extensive testing." In addition, it was determined that the analysis conducted by HFC also did not account for hardware CCF. Any application-specific claims regarding quantification of reliability and availability must demonstrate that the impact of hardware CCF on availability has been addressed in the analysis.

The analysis conducted by HFC does not include a determination of the surveillance interval necessary to support the availability goal for those failures that are only detectable by periodic surveillance. The FMEA performed by HFC concludes that there are no undetectable single failures at the platform level and single failures in the HFC-6000 platform are detected through plant-specific periodic surveillances, diagnostics, anomalous indications, or alarms. In addition, the availability analysis assumes that all single failures of the HFC-6000 platform are detected within one day of occurrence. This assumption implies daily action to address those failures that can only be detected by surveillance. For a specific application based on the HFC-6000 platform, required surveillance methods and testing intervals must be identified. Any application-specific claims regarding quantification of reliability and availability must demonstrate that the impact of surveillance intervals on mean time to repair has been addressed in the analysis.

Although EPRI TR-107330 requires that the availability analysis conform to IEEE Std 352-1987, HFC cites IEEE Std 352-1975, "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Protection Systems," as the basis for its analysis. The evaluation of the HFC-6000 reliability and availability analysis determined that the equations identified by HFC are consistent with the IEEE 352-1987 guidance.

Based on the evaluation, the NRC staff finds that the results of the HFC reliability and availability analysis provide supporting evidence to indicate that the HFC-6000 platform is suitable for use in safety-related applications in a nuclear power plant. However, any application-specific reliability and availability analysis must include the effects of hardware CCF and address the impact of surveillance intervals (see Section 5.2 of this SE).

Based on the reviews identified above, the evaluation indicates the HFC-6000 platform satisfies this requirement. However, because of the dependence of reliability calculations on system configuration (e.g., redundancy), a plant-specific evaluation is necessary to establish full conformance with Clause 5.15. Consideration of software reliability for the HFC-6000 platform is given in Section 3.9.1.9 of this SE.

3.8.3 IEEE STD 603-1991 Clause 6, "Sense and Command Features – Functional and Design Requirements"

The requirements of this clause, in addition to the requirements of Clause 5, apply to the Sense and Command Features of a safety system. The sub-clauses of this requirement are given by the following:

Clause 6.1	Automatic Control
Clause 6.2	Manual Control
Clause 6.3	Interaction between Sense and Command Features and other Systems
Clause 6.4	Deviation of System Inputs
Clause 6.5	Capability for Testing and Calibration
Clause 6.6	Operating Bypass
Clause 6.7	Maintenance Bypass
Clause 6.8	Setpoints

SRP Chapter 7, Appendix 7.1-C, Section 6, "Sense and Command Features - Functional and Design Requirements," provides acceptance criteria for Clause 6.

The functional and design requirements for the sense and command features of a safety system are dependent solely on the specific application. Since the TR does not address a specific application of the platform, include the sensors, nor provide a specific safety system design, the functional and design requirements for a safety system are not available for review and no evaluation of the HFC-6000 platform against these regulatory requirements could be performed.

Although the requirement for setpoints primarily addresses factors beyond the scope of the digital platform (e.g., plant design basis limits, modes of operation, and sensor accuracy), the contribution of the HFC-6000 platform to setpoint uncertainty must be addressed in an application-specific analysis. Since the TR does not document uncertainty calculation parameter values (e.g., hysteresis, drift) associated with the platform, no evaluation of the HFC-6000 platform against this regulatory criterion could be performed. An analysis of accuracy, repeatability, thermal effects, and other necessary data for use in determining the contribution of the HFC-6000 platform to instrumentation uncertainty must be performed as an ASAI (see Section 5.2 of this SE).

3.8.4 IEEE STD 603-1991 Clause 7, "Execute Features – Functional and Design Requirements"

The requirements of this clause, in addition to the requirements of Clause 5, apply to the Execute Features of a safety system. The sub-clauses of this requirement are given by the following:

Clause 7.1	Automatic Control
Clause 7.2	Manual Control

Clause 7.3 Completion of Protective Action
Clause 7.4 Operating Bypass
Clause 7.5 Maintenance Bypass

SRP Chapter 7, Appendix 7.1-C, Section 7, "Execute Features - Functional and Design Requirements," provides acceptance criteria for Clause 7.

The functional and design requirements for the execute features of a safety system are dependent solely on the specific application. Since the TR does not address a specific application of the platform, include the actuators or other execute features, nor provide a specific safety system design, the functional and design requirements for a safety system are not available for review and no evaluation of the HFC-6000 platform against these regulatory requirements could be performed.

Although the requirement for automatic control addresses the execute features are outside the scope of the digital platform, the acceptance criteria guidance in SRP Chapter 7, Appendix 7.1-C, Section 7.1, "Automatic Control," states that the evaluation should also confirm that real-time performance of a digital safety system is deterministic and known. The evaluation of deterministic performance characteristics of the HFC-6000 platform is contained in Section 3.4.2 of this SE and is acceptable for demonstrating that the HFC-6000 platform complies with this requirement.

3.8.5 IEEE STD 603-1991 Clause 8, "Power Source Requirements"

Clause 8 of IEEE Std 603-1991 states that 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, and that specific criteria unique to the Class 1E power systems can be found in IEEE Std 308-1980. This clause also states that for power systems with a degree of redundancy, the safety functions and acceptable reliability must be retained while power sources are in maintenance bypass. SRP Chapter 7, Appendix 7.1-C, Section 8, does not provide acceptance criteria for IEEE Std 603-1991 Clause 8.

Determination of the power sources to be provided to a safety system is an application-specific activity. Since the TR does not address a specific application of the platform, the evaluation against this regulatory requirement is limited to the capabilities and characteristics of the HFC-6000 platform that are relevant for adherence to Clause 8 and its sub-clauses.

Clauses 8.1 and 8.2 address requirements for electrical power sources and non-electrical power sources, respectively. The HFC-6000 platform only uses electrical power and the platform scope does not include the AC power source(s), which is application-specific. Thus, no evaluation of the HFC-6000 platform against these regulatory requirements could be performed.

Clause 8.3 addresses the capability of the safety system to accommodate maintenance bypass of redundant power sources. The HFC-6000 platform employs redundant power supply modules consisting of 24 VDC and 48 VDC assemblies to power the HFC-6000 circuitry and external field devices, respectively. The power supply rack supports two separate AC source connections to allow the redundant power supply modules to be powered by separate power sources. The redundant power, driven by separate power sources, is supplied to the platform modules via separate power traces along the HFC-6000 chassis backplane. Each module of the HFC-6000 platform provides diode auctioneering of the redundant power feeds. Thus, the platform provides suitable capability to enable the safety system to function while one redundant AC power source is failed or in bypass. Based on the results of qualification testing of the HFC-6000 platform under power interruption conditions (see Section 3.3.2 of this SE), HFC committed to define an interface requirement that all installations include two independent power sources for the redundant HFC-6000 power supplies. Based on the HFC commitments for qualification, it is an ASAI to provide two independent AC power sources to separately supply the redundant power supply module groups within the HFC-6000 power supply rack (see Section 5.2 of this SE).

While the evaluation indicates the suitability of the platform to satisfy this requirement, a plant-specific evaluation is necessary to establish full conformance with Clause 8.

3.9 Conformance with IEEE STD 7-4.3.2-2003

RG 1.152, Revision 2, "IEEE Standard Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," states that conformance with the requirements of IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," is a method that the NRC staff has deemed acceptable for satisfying the Commission's regulations with respect to high functional reliability and design requirements for computers used in safety systems of nuclear power plants. SRP Chapter 7, Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std 7-4.3.2," contains guidance for the evaluation of the application of the requirements of IEEE Std 7-4.3.2-2003. This section documents the evaluation of the HFC-6000 platform against this guidance.

The regulatory position in RG 1.152 provides guidance that establishment of a secure environment be addressed in the development process. SRP acceptance criteria for this guidance can be found in SRP Chapter 7, Appendix 7.1-D, Section 9 and DI&C-ISG-01. The evaluation of the HFC-6000 platform against this guidance is contained in Section 3.8 of this SE.

The requirements of IEEE Std 7-4.3.2-2003 supplement the requirements of IEEE Std 603-1991 by specifying criteria that address hardware, software, firmware, and interfaces of computer-based safety systems. Consequently, the structure of IEEE Std 7-4.3.2-2003 parallels that of IEEE Std 603-1991. For those clauses where IEEE Std 7-4.3.2-2003 contains no requirements beyond those found in IEEE Std 603-1991 and SRP Chapter 7, Appendix 7.1-D contains no additional guidance, no review for compliance with IEEE Std 7-4.3.2-2003 is required. Thus, the subsections below are limited to those clauses where further evaluation is warranted. The review against the driving clauses of IEEE Std 603-1991 is documented in the corresponding subsections of Section 3.8 in this SE.

3.9.1 IEEE STD 7-4.3.2-2003 Clause 5, "Safety System Criteria"

Clause 5 of IEEE Std 7-4.3.2-2003 contains requirements beyond those in IEEE Std 603-1991 Clause 5. In addition, SRP Chapter 7, Appendix 7.1-D, Section 5 contains specific acceptance criteria for IEEE Std 7-4.3.2-2003 Clause 5.

The implementation of a computer-based safety system is an application-specific activity. Since the TR does not address a specific application, the evaluation against the following requirements addresses the capabilities and characteristics of the HFC-6000 platform that are relevant for adherence to each requirement.

3.9.1.1 IEEE Std 7-4.3.2-2003 Clause 5.3, "Quality"

Clause 5.3 of IEEE Std 7-4.3.2-2003 states that hardware quality is addressed in IEEE Std 603-1991, and that software quality is addressed in IEEE/EIA Std 12207.0-1996 and supporting standards.

3.9.1.1.1 IEEE STD 7-4.3.2-2003 Clause 5.3.1, "Software Development"

Clause 5.3.1 of IEEE Std 7-4.3.2-2003 requires an approved QA plan consistent with the requirements of IEEE/EIA 12207.0-1996 for all software that is resident at runtime.

EPRI TR-106439, as accepted by the NRC SE dated July 17, 1997, and EPRI TR-107330, as accepted by the NRC SE dated July 30, 1998 provide guidance for the evaluation of existing commercial computers and software.

The operating software of the HFC-6000 platform was dedicated as PDS. Section 3.2.1 of this SE discusses the CGD activities and evidence development undertaken by HFC. The CGD activities included source code inspection, application object testing, component testing, module prototype testing, functional testing, reconstitution of software documentation, and product operating history assessment. The NRC staff also evaluated the quality of the HFC software development process, as it relates to maintaining the PDS, by reviewing the software planning documentation (see Section 3.2.2 of this SE). Based on the evaluation of the CGD evidence and the process in place to preserve the dedication of the PDS, the NRC staff determined that the PDS of the HFC-6000 platform is suitable to support safety-related applications in nuclear power plants and meets this regulatory requirement. However, a plant-specific evaluation of the quality of application software is necessary for future applications.

3.9.1.1.1.1 IEEE STD 7-4.3.2-2003 Clause 5.3.1.1, "Software Quality Metrics"

Clause 5.3.1.1 of IEEE Std 7-4.3.2-2003 states that the use of software quality metrics shall be considered throughout the software life cycle to assess whether software quality requirements are being met.

Since the predeveloped operating software was dedicated rather than developed under the current HFC software QA program, this requirement does not apply within the context of the scope of the TR. An evaluation of metric usage for new software development will be conducted as part of a plant-specific review for any system based on the HFC-6000 platform. It is noted that the responsibilities for the QA manager that are identified in QPP 1.2 (Reference 81) include developing measurable data relating to the effectiveness of the HFC software QA program.

3.9.1.1.2 IEEE STD 7-4.3.2-2003 Clause 5.3.2, "Software Tools"

Clause 5.3.2 of IEEE Std 7-4.3.2-2003 states that software tools used to support software development processes and V&V processes shall be controlled under configuration management, and that the tools shall either be developed to a similar standard as the safety relate software, or that 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.

The software tools used to support the development of the operating software of the HFC-6000 platform are described in Section 3.1.3.4 of this SE. These tools are not subject to formal V&V under the HFC software QA program (Reference 88) but they have been verified through historical usage and their products are required by HFC V&V processes to be subject to sufficient testing to assure that any failure introduced by a tool will be detected. In addition, configuration of these tools is required to be under the SCM program of HFC.

Regarding verification of the tools, the operating software development tools, including the x86 Assembler, Linker and Locator, are Intel products and have been used by HFC more than twenty years. The reliability claims for these development tools are based on the following conditions and/or activities: (1) the stability and verifiability of the language, (2) extensive usage history for the compiler tool, with no recorded compiling errors, (3) extensive usage history of the object code, with no faulted object code reported, and (4) comparison of PC assembler products against original VAX assembler products with no identified discrepancies. Regarding the final item of evidence, a verification process was performed between the original VAX version of the x86 Assembler and current PC based version of the x86 Assembler whenever a retrofit project required a modification of existing HFC-6000 controller software. As part of that verification exercise, no errors were found. Both versions of the development tools involved in the comparisons generated exactly the same executable code.

The NRC staff has reviewed the dedication process for the PDS of the HFC-6000 platform and the verification evidence for the operating software development tools in this section and in Section 3.2.1 of this SE. Based on the comparison of object code, the historical usage of the development tools, and the verification of the PDS under the dedication effort, the NRC staff has determined that the output of the software development tools for operating software of the HFC-6000 platform was subject to V&V activities that would detect any defects or errors caused by the usage of the tools. Consequently, the use of these tools in the development of the platform software is consistent with this regulatory criterion and is, therefore, acceptable.

3.9.1.1.3 IEEE STD 7-4.3.2-2003 Clause 5.3.3, "Verification and Validation"

Clause 5.3.3 of IEEE Std 7-4.3.2-2003 states that a V&V program exists throughout the system life cycle, and states that the software V&V effort be performed in accordance with IEEE Std 1012-1998.

As noted, the operating software of the HFC-6000 platform was predeveloped before the HFC software QA program was established. Consequently, the PDS was commercially dedicated and did not always have the current V&V program in place. The V&V activities employed in the dedication process for the PDS (see Sections 3.2.1.1.1, 3.2.1.1.3, 3.2.2.10.3, and 3.2.2.9), such as code inspection, software component testing, requirements traceability analysis, and software hazard analysis, serve to indicate the suitability of the V&V that was applied to the dedicated PDS. In addition, the HFC software QA program was reviewed as it applies to maintenance of the PDS (see Section 3.2.2 of this SE). As a result of these reviews, the NRC staff finds the V&V of the HFC-6000 platform meets this regulatory criterion.

3.9.1.1.3.1 Software Testing

RG 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std 829-1983, "IEEE Standard for Software Test Documentation," subject to the provisions and exceptions identified in the RG, identifies an acceptable method for satisfying test documentation requirements.

RG 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std 1008-1987, "IEEE Standard for Software Unit Testing," subject to the provisions and exceptions identified in the RG, identifies an acceptable method for satisfying software unit testing requirements.

As noted, the operating software of the HFC-6000 platform was predeveloped before the HFC software QA program was established. Consequently, the PDS was commercially dedicated and did not have the current software testing processes under the HFC V&V program in place. Nevertheless, the testing that was conducted as part of the CGD process included white box (step-by-step execution of the operating software code, application software object testing, software component testing, prototype testing, and functional testing (see Section 3.2.1.1 of this SE). Based on evaluation of this testing regime, the NRC staff concludes that the software testing of the PDS of the HFC-6000 platform is consistent with the cited guidance on testing and is, therefore, acceptable to meet this regulatory criterion.

3.9.1.1.4 IEEE STD 7-4.3.2-2003 Clause 5.3.4, "Independent V&V Requirements"

Clause 5.3.4 of IEEE Std 7-4.3.2-2003 defines the levels of independence required for the V&V effort, in terms of technical independence, managerial independence, and financial independence.

The independence provided by the V&V activities and QA organization for the HFC software QA program is discussed in Sections 3.2.2.1, 3.2.2.3, and 3.2.2.10.1 of this SE. Based on these reviews, the NRC staff finds that the independence of V&V applied to the HFC-6000 platform meet this regulatory criterion.

3.9.1.1.5 IEEE STD 7-4.3.2-2003 Clause 5.3.5, "Software Configuration Management"

Clause 5.3.5 of IEEE Std 7-4.3.2-2003 states that Software configuration management shall be performed in accordance with IEEE Std 1042-1987, and that IEEE Std 828-1998 provides guidance for the development of software configuration management plans. IEEE Std 828-1990 and IEEE Std 1042-1987 are endorsed by RG 1.169.

The SCM of software components and the integrated PDS of the HFC-6000 platform was discussed in Section 3.2.2.11 of this SE. Based on this review, the NRC staff determined that the SCMP of the HFC software QA program, as applied to the control and maintenance of the PDS of the HFC-6000 platform, complies with this regulatory criterion and is, therefore, acceptable.

3.9.1.1.6 IEEE STD 7-4.3.2-2003 Clause 5.3.6, "Software Project Risk Management"

Clause 5.3.6 of IEEE Std 7-4.3.2-2003 defines the risk management (RM) required for a software project. SRP Chapter 7, Appendix 7.1-D, Section 5.3.6, "Software Project Risk Management" provides acceptance criteria for software project RM. This section states that software project RM is a tool for problem prevention, and be performed at all levels of the digital system project to provide adequate coverage for each potential problem area. It also states that 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. Additional guidance on the topic of RM is provided in IEEE/EIA Std 12207.0-1996, "IEEE Standard for Industry Implementation of International Standard ISO/IEC 12207: 1995 (ISO/IEC 12207) Standard for Information Technology – Software Life Cycle Processes," and IEEE Std 1540-2001, "IEEE Standard for Life Cycle Processes B Risk Management."

The SMP and SDP establish the requirement for a project risk assessment (see Sections 3.2.2.1 and 3.2.2.2 of this SE). The SSP and SVVP require criticality, hazard, security, and risk analyses for each life cycle phase (see Sections 3.2.2.9 and 3.2.2.10.1 of this SE). As an example, the development plan for the ERD111 qualification project (Reference 85) contains a risk assessment for the project to generically qualify the HFC-6000 platform. Additionally, the initial submitted versions of the reconstituted requirements specification for the operating software and IOM software (References 94 and 95, respectively) each document findings from module level safety analyses for the PDS, which also include risk analyses. Finally, the module specification for the controller firmware, MS901-000-01 (Reference 30), documents design features for the controller module that mitigate the identified hazards and risks as well as addressing means to support security. These software development and management plans address development, safety, and security risks throughout the life cycle, and these plans include the development and use of the HFC-6000 platform. The NRC staff has reviewed the software life cycle planning documents (see Section 3.2.2 of this SE) and the design output documents (see Section 3.2.3 of this SE) and determined that the HFC-6000 platform complies with Clause 5.3.6 of IEEE Std 7-4.3.2-2003. Development of future applications should still use a software risk management program to assist in the identification and resolution of potential problems.

3.9.1.2 IEEE STD 7-4.3.2-2003 Clause 5.4, "Equipment Qualification"

Clause 5.4 of IEEE Std 7-4.3.2-2003 defines the computer equipment qualification required for a software project. SRP Chapter 7, Appendix 7.1-D, Section 5.4, "Equipment Qualification," provides acceptance criteria for computer equipment qualification. This section of Appendix 7.1-D states that in addition to the equipment qualification criteria provided by IEEE Std 603-1991 and Section 5.4 of SRP Chapter 7, Appendix 7.1-C, additional criteria, as defined in Sections 5.4.1 and 5.4.2, are necessary to qualify digital computers for use in safety systems. These sections are discussed below.

3.9.1.2.1 IEEE STD 7-4.3.2-2003 Clause 5.4.1, "Computer System Testing"

Clause 5.4.1 of IEEE Std 7-4.3.2-2003 discusses the software that should be operational on the computer system while qualification testing is being performed. SRP Chapter 7, Appendix 7.1-D, Section 5.4.1, "Computer System Testing," provides acceptance criteria for computer equipment qualification testing. This section states that computer equipment qualification testing should be performed while the computer is functioning, with software and diagnostics that are representative of those used in actual operation.

Section of this SE discusses the evaluation of the environmental qualification program for the HFC-6000 platform. In particular, HFC complied with the guidance of EPRI TR-107330 for the generic qualification of a PLC platform. EPRI TR-107330, Section 6.2.2, "Test Specimen Application Program Configuration Requirements," specifies development of a synthetic application program to verify the PLC functionality under the full range of service conditions (i.e., normal conditions as well as environmental extremes). In addition, Table 5.1 of EPRI TR-107330 specifies the testing conditions under which specific tests must be executed. Section 3.3.1 of this SE discusses the TSAP developed by HFC for its generic qualification program. The TSAP was specifically designed to support qualification testing of the HFC-6000 platform while providing functionality representative of safety-related applications.

Based on evaluation in Section 3.3 of this SE and review of the design documents for the TSAP (References 109 and 110) as well as qualification test plans and procedures (References 76, 77, 79, 107, 111 through 120), the NRC staff concludes that the HFC qualification program met the requirement for computer testing of the HFC-6000 platform, subject to the satisfactory resolution of the generic open items in Section 5.1 of this SE.

3.9.1.2.2 IEEE STD 7-4.3.2-2003 Clause 5.4.2, "Qualification Of Existing Commercial Computers"

Clause 5.4.2 of IEEE Std 7-4.3.2-2003 defines the Qualification of Existing Commercial Computers for use in safety-related applications in nuclear power plants. SRP Chapter 7, Appendix 7.1-D, Section 5.4.2, "Qualification of Existing Commercial Computers," provides acceptance criteria for computer equipment qualification. This section states that EPRI TR-106439 and EPRI TR-107330 provide specific guidance for the evaluation of commercial grade digital equipment and existing PLCs.

HFC commercially dedicated the predeveloped operating software of the platform under the guidance of EPRI TR-106439 and generically qualified the HFC-6000 platform in accordance with the guidance of EPRI TR-107330. The evaluation of the evidence from each of these activities is contained in Sections 3.2.1 and 3.3, respectively, of this SE. Based on the findings of this review, the NRC staff finds that the generic qualification program of the HFC-6000 platform complies with the guidance of both EPRI TR-106430 and EPRI TR-107330, subject to satisfactory resolution of the generic open items in Section 5.1 of this SE.

3.9.1.2.2.1 IEEE STD 7-4.3.2-2003 Clause 5.4.2.1, "Preliminary Phase of the Cots Dedication Process"

This clause of IEEE Std 7-4.3.2-2003 specifies that the risks and hazards of the dedication process are to be evaluated, the safety functions identified, configuration management established, and the safety category of the system determined. Most of these requirements are satisfied generically by the approved guidance in EPRI 0TR-107330, which addressed the risks and hazards in the development of the guide and selected the safety functions and system safety categories that are covered by the scope of the guidance.

The configuration management of the COTS item (i.e., the HFC-6000 platform) is provided by HFC under its SCMP, which is discussed in Section 3.2.2.11 of this SE. Based on the prior acceptance of the EPRI TR-107330 guidance and the review of the HFC SCMP, the NRC staff finds that the HFC qualification program met the requirements of this clause (and its sub-clauses on risks and hazards evaluation, safety function identification, and configuration management controls) for the computer qualification of the HFC-6000 platform.

3.9.1.2.2.2 IEEE STD 7-4.3.2-2003 Clause 5.4.2.2, "Detailed Phase of the Cots Dedication Process"

This clause of IEEE Std 7-4.3.2-2003 involves evaluation of the commercial grade item for acceptability based on detailed acceptance criteria. In particular, critical characteristics of the COTS item are to be evaluated and verified. The characteristics are identified in terms of physical, performance, and development process attributes. This requirement is addressed by the guidance in EPRI TR-106439. Specifically, a critical design review is specified to identify physical, performance, and dependability (i.e., development process) characteristics, which are then verified by one or more of the fours methods identified in the guide.

Section 3.2.1 of this SE contains the evaluation of the COTS dedication process executed by HFC for the predeveloped operating software of the HFC-6000 platform. As discussed, a commercial grade software evaluation was performed by HFC to identify critical characteristics. A survey of the QA processes in place during the development of the legacy software was coupled with testing to verify that the critical characteristics are acceptably demonstrated by the HFC-6000 platform. In particular, application object tests, software component tests, prototype tests, functional tests, and qualification tests were performed to demonstrate acceptable quality for the CGD of the PDS. Based on the review of the dedication process and the testing results, the NRC staff determined that the HFC qualification program satisfies this clause for the generic qualification and CGD of the HFC-6000 platform.

3.9.1.2.2.3 IEEE STD 7-4.3.2-2003 Clause 5.4.2.3, "Maintenance of Commercial Dedication"

This clause of IEEE Std 7-4.3.2-2003 specifies that documentation supporting CGD of a computer-based system or equipment is to be maintained as a configuration control item. In addition, modifications to dedicated computer hardware, software, or firmware are to be traceable through formal documentation.

The HFC qualification program has generated and maintained evidence of CGD and qualification for the HFC-6000 platform. Section 3.2.2.11 of this SE discusses HFC's approach to configuration control under its SCMP. Section 3.2.2 describes the plans and procedures for treating safety-related software under the HFC software QA program. In particular, Section 3.2.2.6 addresses the SMaintP and the CAP process in place to ensure traceable, high-quality maintenance activities. Based on the review of the HFC software QA program for its suitability to preserve the dedication of the PDS under maintenance modification, the NRC staff finds that the HFC software QA program meets this requirement as applied to maintenance of the PDS of the HFC-6000 platform.

3.9.1.3 IEEE STD 7-4.3.2-2003 Clause 5.5, "System Integrity"

Clause 5.5 of IEEE Std 7-4.3.2-2003 states that in addition to the system integrity criteria provided by IEEE Std 603-1991, the digital system shall be designed for computer integrity, test and calibration, and fault detection and self diagnostics activities. These attributes are further defined in Clause 5.5.1, "Design for computer integrity," Clause 5.5.2, "Design for test and calibration," and Clause 5.5.3, "Fault detection and self diagnostics." There are no specific acceptance criteria shown in SRP Chapter 7, Appendix 7.1-D, Section 5.5, "System Integrity."

3.9.1.3.1 IEEE STD 7-4.3.2-2003 Clause 5.5.1, "Design for Computer Integrity"

Clause 5.5.1 of IEEE Std 7-4.3.2-2003 states that the computer must be designed to perform its safety function when subjected to conditions, either external or internal, that have significant potential for defeating the safety function.

The HFC-6000 platform provides redundant controllers, redundant network connections, redundant bus links to I/O modules, and redundant power supplies. The redundant features of the HFC-6000 are described in Section 3.1.1 of this SE. The use of redundancy provides fault tolerant capabilities which, coupled with diagnostics and self-testing as discussed in Section 3.4.3 of this SE, can facilitate a high-level of computer integrity. Furthermore, the computer qualification activities documented by HFC, which are discussed in Sections 3.9.1.2.2, 3.2.1 and 3.3, provide suitable evidence that the HFC-6000 platform is capable of handling conditions, external or internal, that have the potential to defeat implemented safety functions. Specifically, the NRC staff reviews of the platform capability to withstand single failures in Section 3.8.2.1 of this SE, the demonstration of environmental withstand (subject to noted generic open items) in Section 3.3, and the provisions for security in Section 3.6, support the determination that the HFC-6000 platform is suitable for conforming to Clause 5.5.1.

3.9.1.3.2 IEEE STD 7-4.3.2-2003 Clause 5.5.2, "Design for Test and Calibration"

Clause 5.5.2 of IEEE Std 7-4.3.2-2003 states that test and calibration functions shall not adversely affect the ability of the computer to perform its safety function, and that it shall be verified that the test and calibration functions do not affect computer functions that are not included in a calibration change. The clause further states that V&V, configuration management, and QA be required for test and calibration functions on separate computers such as test and calibration computers that provide the sole verification of test and calibration data, but that V&V, configuration management, and QA is not required when the test and calibration function is resident on a separate computer and does not provide the sole verification of test and calibration data for the computer that is part of the safety system.

Determination of the test and calibration requirements that must be fulfilled depends upon the plant-specific safety requirements that apply and establishment of the types of surveillance necessary for the safety system to ensure that the identifiable single failures only announced through testing are detected are application-specific activities. Since the TR does not address a specific application or establish a definitive safety system design, the evaluation against this requirement is limited to consideration of the means provided within the platform to enable testing and calibration of an implemented system.

Online diagnostics and self-tests are provided by the HFC-6000 to support test and calibration requirements in general. The methods for calibration of HFC-6000 IOM in the field are not within the scope of the TR so this capability is not reviewed in this SE. As noted in Section 3.8.2.7 of this SE, automatic calibration checks are provided for the AI modules to correct for drift of the data acquisition circuitry. The qualification tests performed for the HFC-6000 platform were conducted with diagnostics executing in conjunction with a synthetic application program simulating safety functions (see Section 3.3.1 of this SE). The performance of these tests demonstrated that the diagnostics and self-tests did not adversely affect the ability of the computer to perform its simulated safety functions. Therefore, the NRC staff concludes that the diagnostic and self-test capabilities provided by the HFC-6000 platform conform to this requirement.

3.9.1.3.3 IEEE STD 7-4.3.2-2003 Clause 5.5.3, "Fault Detection and Self-Diagnostics"

Clause 5.5.3 of IEEE Std 7-4.3.2-2003 discusses fault detection and self diagnostics, and stated that if reliability requirements warrant self diagnostics, then computer programs should contain functions to detect and report computer system faults and failures in a timely manner, and that these self diagnostic functions shall not adversely affect the ability of the computer system to perform its safety function, or cause spurious actuations of the safety function.

The software-based HFC-6000 diagnostics and self-test capabilities offer extensive and thorough coverage of the identified failure modes from the FMEA performed by HFC (see Sections 3.4.3 and 3.8.2.1 of this SE for discussions of diagnostic and test software and the HFC FMEA, respectively). However, it is recognized that diagnostics and software watchdog timers may fail. Consequently, the HFC-6000 platform provides onboard hardware watchdog timers for each module (i.e., controller and I/O) as a failsafe response to failed software execution or processor stall.

The watchdog timer is implemented strictly by hardware components and will reset if a strobe pulse is not received within a specified interval. Every context switch interval (i.e., predefined execution cycle), a utility is called to produce an output strobe pulse for the watchdog timer. This utility is only executed if the health condition of the module indicates that the software execution and processor (main and subordinate) status are acceptable or "sane." Not only does the hardware watchdog timer address processor stall or application software termination, it is also capable of responding to incomplete execution of the safety function. A key condition that the watchdog utility can check before generating the strobe pulse is whether a flag is set confirming the successful execution of the safety function (i.e., application program) at least once during a context switch interval.

The hardware-based diagnostic features of the HFC-6000 platform satisfy this requirement and, along with the software-based diagnostics, the HFC-6000 platform is acceptable for providing fault detection in support of safety-related applications. However, because the FMEA identified failures that are not automatically detected but instead require operator surveillance, there may be additional fault-detection and diagnostic capabilities implemented as part of the application or system design to provide more comprehensive coverage of identified failures with automatic tests and diagnostics. Therefore, a plant-specific evaluation is necessary to establish full conformance with Clause 5.5.3.

3.9.1.4 IEEE STD 7-4.3.2-2003 Clause 5.6, "Independence"

Clause 5.6 of IEEE Std 7-4.3.2-2003 states that, in addition to the requirements of IEEE Std 603-1991, data communications between safety channels or between safety and nonsafety systems shall not inhibit the performance of the safety function. SRP Chapter 7, Appendix 7.1-D, Section 5.6, "Independence," provides acceptance criteria for computer equipment qualification. This section states that the regulation at 10 CFR Part 50, Appendix A, GDC 24, "Separation of protection and control systems," requires 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.

Establishment of communications among redundant portions of a safety system or between the safety system and other nonsafety systems in a plant is an application-specific activity. The base platform architecture identified in the TR does not specify any direct connections or bi-directional communications between the HFC-6000 platform and any other system. Since the TR does not address a specific application or provide a definitive safety system design, the evaluation of the HFC-6000 platform against the communications independence aspect of this regulatory requirement is limited to features and capabilities of its communication networks.

The description of the communications interconnections for the HFC-6000 platform is contained in Sections 3.1.2 and 3.5.1 of this SE. Sections 3.1.3.2.3 and 3.1.3.2.4 of this SE describe the software features of the ICL and C-Link protocols while Sections 3.4.2 and 3.4.3 discuss their deterministic performance characteristics and diagnostic capabilities. Section 3.5.1 of this SE discusses communications interconnects within the scope of the HFC-6000 platform while 3.5.2 contains the evaluation of the HFC-6000 communications capabilities with respect to the guidance in DI&C-ISG-04. Section 3.6.3.2 of this SE addresses security design access control for the HFC-6000 platform. As discussed in these sections, both the ICL and C-Link provide features to promote reliable, deterministic communications capabilities to support high-integrity communications. A key feature of the HFC-6000 platform approach to communications is the use of a buffered circuit concept with interposing communications processors for both C-Link and ICL communications. In each case, a separate, dedicated, onboard processor (i.e., the C-Link and ICL processors) performs the communication function of the HFC-SBC06 controller module. Data exchange among the processors is conducted through shared memory access. Consequently, the system processor, and thus the execution of the safety function, is isolated from the management of the communication functions.

As an additional feature to support communications independence for nuclear safety applications, HFC design practice restricts communication over the C-Link to broadcast-only messages. Additionally, an isolated, unidirectional gateway is intended to be used for any communications link to nonsafety systems over the C-Link. Since the gateway is not part of the base platform, credit for this feature in promoting communications independence depends on an ASAI to verify that the gateway provides strictly unidirectional communication (i.e., receive only) and does not transmit across the C-Link (see Section 5.2 of this SE). In addition, an ASAI is required to ensure that any device installed as a node on the safety C-Link as an interface to nonsafety systems or networks fulfills electrical, physical, and communications independence requirements (see Section 5.2 of this SE).

Based on the evaluation described in this section and the other referenced sections, the NRC staff finds that the communications capabilities of the HFC-6000 platform for I/O data transfer across the ICL and broadcast messaging across the C-Link provide acceptable design features to enable communications independence when appropriately configured. However, the specific interconnections defined for an application must be determined and evaluated in a plant-specific review.

3.9.1.5 IEEE STD 7-4.3.2-2003 Clause 5.7, "Capability for Test and Calibration"

Clause 5.7 of IEEE Std 7-4.3.2-2003 states that there are no requirements beyond those found in IEEE Std 603-1991. SRP Chapter 7, Appendix 7.1-D, Section 5.7, "Capability for Test and Calibration," provides no acceptance criteria for IEEE Std 7-4.3.2-2003 Clause 5.7.

As described in Sections 3.8.2.7, 3.9.1.3.2, and 3.9.1.3.3 of this SE, the HFC-6000 platform provides on-line diagnostics and self-tests to detect failures within the platform. Hardware watchdog timers are also provided to provide an additional fault detection in the event that the on-line diagnostics or self-tests fail.

The NRC staff finds that the HFC-6000 platform complies with this clause. However, as was noted in Section 3.8.2.7, it is an ASAI to identify that the diagnostics and self-tests do address the failure modes of the specific application and that appropriate display mechanisms are provided.

3.9.1.6 IEEE STD 7-4.3.2-2003 Clause 5.8, "Information Displays"

Clause 5.8 of IEEE Std 7-4.3.2-2003 states that there are no requirements beyond those found in IEEE Std 603-1991. However, SRP Chapter 7, Appendix 7.1-D, Section 5.8, "Information Displays," noted that, in the past, information displays only provided a display function and, therefore, required no two way communication. More modern display systems may also have included control functions and, therefore, the NRC staff reviews the capacity for information displays to ensure that incorrect functioning of the information displays does not prevent the safety function from being performed when necessary.

Since the TR does not address a specific application nor include display devices within its scope, no evaluation of the HFC-6000 platform against this clause could be performed.

3.9.1.7 IEEE STD 7-4.3.2-2003 Clause 5.9, "Control Of Access"

Clause 5.9 of IEEE Std 7-4.3.2-2003 states that there are no requirements beyond those found in IEEE Std 603-1991. For this reason, there is no additional guidance beyond that found in Section 5.9 of SRP Chapter 7, Appendix 7.1-C and RG 1.152, Revision 2.

The regulatory position section in RG 1.152, Revision 2, provides guidance on security regarding electronic access to a safety system. SRP acceptance criteria for this guidance can be found in SRP Chapter 7, Appendix 7.1-D, Section, Section 9 and DI&C-ISG-01. The evaluation of the HFC-6000 platform against this guidance is contained in Section 3.6 of this SE.

3.9.1.8 IEEE STD 7-4.3.2-2003 Clause 5.11, "Identification"

Clause 5.11 of IEEE Std 7-4.3.2-2003 states that (1) identification requirements specific to software systems (i.e., firmware and software identification) shall be used to assure the correct software is installed in the correct hardware component, (2) means shall be included in the software such that the identification may be retrieved from the firmware using software maintenance tools, and (3) physical identification requirements of the digital computer system hardware shall be in accordance with the identification requirements in IEEE Std 603-1991 Clause 5.11. SRP Chapter 7, Appendix 7.1-D, Section 5.11, "Identification" provides acceptance criteria and adds that 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 for computer equipment qualification.

Establishing software/firmware identification requirements and providing the means for retrieving that identification information are directly related to the HFC QA Program. HFC-6000 software is regulated by the HFC SCM procedures and WIs (References 89 and 90). Section 3.2.2.11 contains the evaluation of the HFC SCMP as it applies to maintaining PDS. The HFC SCMP for application software is outside of the scope of this review.

HFC-6000 source code is an identified SCM component so version management and change control mechanisms are applied. The platform software components for the HFC-6000 are controlled based on assigned part numbers. The configuration information of each software component is securely maintained as part of the HFC system configuration management records and can be referenced by part number against a BOM for a specific project. Software versions for the assemblage of software components are defined in terms of a formally released, configuration controlled software project. The source code for each software version is stored in an access-controlled repository. The complied system software for each processor contains embedded information with build date, firmware type, and an internal checksum. This compiled software is burned into PROMs using access-controlled equipment as part of the manufacture and assembly activities. No mechanism is provided by HFC for altering the system software of a module in the field other than replacement of the onboard PROMs.

Identification of the system software can be checked at the factory using the development tools maintained by HFC. The physical labeling applied to a module identifies the version and part number of the installed firmware, which can be crosschecked against the BOM to determine the corresponding build date and checksum. Comparison of this information against the checksum and build date read from the system software resident in firmware allows confirmation that the correct software is installed. The process for confirming the identification of installed firmware was observed by NRC staff during the regulatory audits conducted at the HFC facility (References 15 and 16).

Based on this evaluation and the findings regarding hardware identification in Section 3.8.2.11 of this SE, the NRC staff determined that the HFC-6000 platform complies with the guidance of IEEE Std 7-4.3.2-2003 Clause 5.11 for its system software. Evaluation of application software is outside the scope of this review and will be addressed as part of an application-specific review.

3.9.1.9 IEEE STD 7-4.3.2-2003 Clause 5.15, "Reliability"

Clause 5.15 of IEEE Std 7-4.3.2-2003 states that, in addition to the requirements of IEEE Std 603-1991, when reliability goals are identified, the proof of meeting the goals shall include the software. Guidance is provided in SRP Chapter 7, Appendix 7.1-C, Section 5.15.

As stated in RG 1.152, Revision 2, the NRC does not endorse the concept of quantitative reliability goals as the sole means of meeting the Commission's regulations for reliability of digital computers in safety systems. Quantitative reliability determination, using a combination of analysis, testing, and operating experience, can provide an added level of confidence in the reliable performance of the computer system.

Determination of the reliability of a digital safety system is an application-specific activity that requires an assessment of a full system design, its application and system software, and the software life cycle processes. Since the TR does not address a specific application, establish a definitive safety system design, nor identify any plant I&C architectures, the evaluation against this requirement is limited to consideration of the reliability characteristics of the digital platform and the quality of its system software. While the evaluation indicates the platform satisfies this requirement, a plant-specific evaluation is necessary to establish full conformance with Clause 5.15. Evaluation of the hardware reliability for the HFC-6000 platform is given in Section 3.8.2.15 of this SE.

HFC performed a quantitative reliability and availability analysis for the HFC-6000 platform (see Section 3.8.2.15 of this SE) as specified by EPRI TR-107330. According to EPRI TR-107330, software failures are generally not determined quantitatively because they "are caused by design errors and; therefore, do not follow the random failure behavior used for hardware reliability analysis." Thus, the reliability and availability analysis results are not sufficient as a sole means for evaluating reliability of digital safety systems based on the HFC-6000 platform.

A qualitative evaluation of software reliability for a safety system involves consideration of the quality of the software as demonstrated through its life cycle processes, testing, and operating experience. Application software and its specific life cycle processes are outside the scope of this review and will be treated in an application-specific review. The platform software for the HFC-6000 has undergone commercial grade dedication as predeveloped software and the associated development history, operating experience, life cycle documentation, and testing and review activities have been reviewed (see Section 3.2 of this SE). Specifically, HFC performed an analysis of the reliability of the PDS of the HFC-6000 platform (see Section 3.2.1.3 of this SE). Based on their assumptions of the full applicability of the total module operating years that are cited for the predecessor product lines, an estimated 80 percent duty cycle for each implementation, and an identification of only one critical defect in the historical performance records, HFC determined in their analysis that the defects per hour were on the order of 10^{-6}, as reported in Section 10.1.4 of the TR. The evaluation by the NRC staff finds that the assumptions underlying the HFC quantitative analysis appear to be unsubstantiated (by reliable data). Nevertheless, the NRC staff's evaluation finds the dedication evidence for the PDS of the HFC-6000 platform to show sufficient quality to indicated acceptable reliability for the platform software. In addition, the HFC software maintenance processes provide confidence that reliable safety-related software can be implemented in systems based on the HFC-6000 platform (see Section 0 of this SE). The demonstrated qualitative evidence of the operating software reliability for the HFC-6000 platform shows that the PDS provides suitable reliability and meets this requirement. However, demonstration of the hardware and software reliability of the implemented system is necessary to fully comply with this clause for digital safety system reliability. Specifically, an evaluation of system reliability, including the contribution of application software, will be treated in a plant-specific review.

4.0 SUMMARY

This SE discusses the acceptability of the HFC-6000 platform for use as the basis for a safety-related digital I&C system in nuclear power plants. Each of the findings or conclusions summarized below may be subject to the satisfactory resolution of generic open items identified in the foregoing sections and documented in Section 5.1 of this SE. Careful attention must also be given to the plant-specific items listed in Section 5.2 of this SE.

The GDC listed in Appendix A to 10 CFR Part 50 establish the minimum requirements for the design of nuclear power plants; 10 CFR 50.55a(h) incorporates IEEE Std 603-1991. The RGs and endorsed industry codes and standards listed in the SRP, Table 7-1, are the guidelines used as the fundamental basis for this evaluation. Satisfaction of the applicable regulatory requirements can only be fully established in the context of a specific application implemented in a particular system design. Section 2.2 of this SE refines the basis for this review by identifying the regulatory criteria that are applicable to the review of a generic platform for use in safety-related applications in nuclear power plants. In particular, the determination of relevant regulations and guidance expressed in that section of this SE addressed the scope of the HFC-6000 platform as defined in the TR. This section of this SE discusses the acceptability of the HFC-6000 platform as it applies to these regulatory requirements.

The regulation at 10 CFR 50.55a(a)(1), "Quality Standards for Systems Important to Safety," is addressed by conformance with the codes and standards listed in the SRP. As identified in Section 8.5 of the TR, HFC employed codes, standards, and commercial-grade dedication guidance in the development of the HFC-6000 platform that are the same as or equivalent to the standards identified in the SRP. For the systems and components reviewed, the NRC staff concludes that HFC adequately identified the guidelines applicable to safety-related systems that are the target for application of the platform. Based upon the review of the HFC-6000 design approaches for compliance with the guidelines, the NRC staff concludes that the requirements of GDC 1 and 10 CFR 50.55a(a)(1) have been met, subject to closure of generic open items and licensees addressing ASAIs.

The regulation at 10 CFR 50.55a(h), "Protection and safety systems," incorporates the requirements of IEEE Std 603-1991, which addresses both system-level design issues and quality criteria for qualifying systems for safety applications. HFC has addressed these issues in the TR. Subject to the limitations of this SE, the NRC staff finds that the HFC-6000 platform meets the criteria of IEEE Std 603-1991 and the supplemental standard IEEE Std 7-4.3.2-2003 at the platform level and its features and characteristics, as discussed in this SE, is capable of supporting full conformance with regulations at the system level. For the modules and components reviewed, the NRC staff concludes that the HFC-6000 platform is in compliance with this requirement subject to closure of generic open items and licensees addressing ASAIs.

The NRC staff has reviewed the requirements of IEEE Std 603-1991, and finds that Clauses 5.1, 5.3, 5.4, 5.6, 5.7, 5.9, 5.10, 5.11, and 5.15 apply. The NRC staff has determined that the HFC-6000 platform complies with the requirements of 10 CFR 50.55a(h) with regard to IEEE Std 603-1991.

The review included the identification of those systems and components for the HFC-6000 platform designed to survive the effects of earthquakes, other natural phenomena, abnormal environments and missiles. On the basis of this review and pending satisfactory resolution of the generic open items identified in Section 5.1 of this SE, the NRC staff concludes that the HFC-6000 platform has demonstrated adequate qualification for general use in safety-related applications consistent with the design bases for those safety related systems, subject to confirmation that the established qualification envelope bounds the plant-specific environmental conditions. Therefore, the NRC staff finds that the identification of these modules and components satisfies the requirements of GDC 2 and 4.

Based on the review of safety system status information and provisions to support safe shutdown for the modules and components reviewed, the NRC staff concludes that capabilities are present to enable information to be provided to monitor the safety-related applications over the anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety. The HFC-6000 platform also provides capabilities to appropriately support actions to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions. Therefore, the NRC staff finds that the HFC-6000 platform design satisfies the requirements of GDC 13.

Based on the review of potential system functions, for the modules and components reviewed, the NRC staff concludes that the HFC-6000 platform can comply with the design bases requirements of IEEE Std 603-1991. On the basis of its review, the NRC staff concludes that a safety system based on the HFC-6000 platform can include the provision to detect accident conditions and anticipated operational occurrences in order to initiate reactor shutdown consistent with the accident analysis presented in Chapter 15 of the SAR of a nuclear power plant. Therefore, the NRC staff finds that the

HFC-6000 platform complies with the requirements of GDC 20. However, licensee evaluation of plant-specific accident analyses is necessary.

The HFC-6000 platform can support fulfillment of the guidelines for test and calibration capabilities and comply with the guidelines on the application of the single-failure criterion. On the basis of this review, the NRC staff concludes that, for the modules and components reviewed, the HFC-6000 platform complies with the requirements of IEEE Std 603-1991 with regard to system reliability and testability. Therefore, the NRC staff finds that the HFC-6000 platform meets the requirements of GDC 21.

The HFC-6000 platform support compliance with the guidelines for protection system independence for installed systems based on the platform. On the basis of its review, the NRC staff concludes that, for the modules and components reviewed, the HFC-6000 platform complies with the requirements of IEEE Std 603-1991 with regard to system independence. Therefore, the NRC staff concludes that the HFC-6000 platform meets the requirements of GDC 22.

On the basis of its review of the FMEA submitted by HFC, the NRC staff concludes that the HFC-6000 platform can support design approaches that are consistent with the requirements of GDC 23. Therefore, the NRC staff finds that, for the modules and components reviewed, system design approaches to be implemented with the HFC-6000 platform can satisfy the requirements of GDC 23. Plant-specific FMEAs will be required for any implementation of the HFC-6000 platform (see Section 5.2 of this SE).

On the basis of its review of the reports of the dedication of commercial-grade operating software of the HFC-6000 hardware and software for use in nuclear safety systems, the NRC staff concludes that the HFC-6000 platform follows the guidance in EPRI TR-106439 and is, therefore, acceptable.

On the basis of the review of the HFC software QA program for the maintenance of PDS, the NRC staff concludes that the QAPM specifies plans that will provide a quality software life cycle process, and that these plans commit to documentation of life cycle activities that will permit the NRC staff or others to evaluate the quality of the design features being maintain upon which a safety determination may be based. The NRC staff, therefore, concludes that the software development plan for maintenance of dedicated PDS of the HFC-6000 platform meets the guidance of RG 1.152 and that the special characteristics of computer systems, including security, have been adequately addressed at the platform level. Based on its review, the NRC staff finds, therefore, that the HFC-6000 platform meets the requirements of GDC 1 and 21.

The NRC staff concludes that the HFC-6000 platform meets the requirements of 10 CFR 50.55a(a)(1) and 55a(h). It also meets GDC 1, 2, 4, 13, and 20-24, and IEEE Std 603-1991 for the design of safety-related reactor protection systems, engineered safety features systems, and other plant systems, as well as the guidelines of RG 1.152 and supporting industry standards for the design of digital systems.

5.0 LIMITATIONS AND CONDITIONS

On the basis of the review documented in this SE, the NRC staff concludes that the HFC-6000 platform is acceptable for use in the development, installation, and operation of safety-related systems in nuclear power plants, pending acceptable resolution of the generic open items identified in Section 5.1 of this SE and subject to the plant-specific conditions and limitations listed in Section 5.2 of this SE.

5.1 Generic Open Items

On the basis of its review of the HFC-6000 platform, the NRC staff has identified the following generic open items, which must be resolved to establish acceptability of the platform for general use in implementing safety-related applications at nuclear power plants. The principal generic open item relates to adequately demonstrating environmental qualification of the HFC-6000 platform for environmental stress and EMC. The subsequent open items constitute corresponding elements of the HFC qualification program that require further evidence to acceptably demonstrate qualification of the platform in terms of performance characteristics and the testing envelope.

1. HFC has committed to conducting a retest of both environmental stress withstand and EMI/RFI immunity capabilities of the HFC-6000 platform to demonstrate generic environmental qualification for temperature and humidity exposure and EMC (Reference 106). Submission of additional testing results or other comparable evidence for review is necessary to demonstrate environmental qualification of the HFC-6000 platform under the generic environmental and EM service conditions defined in EPRI TR-107330. The NRC staff review of environmental qualification of the HFC-6000 platform is discussed in Section 3.3 of this SE.

2. The qualification testing conducted for the HFC-6000 platform does not establish qualification of the hardware watchdog timer for the HFC-SBC06 controller module under the service conditions defined in EPRI TR-107330. Submission of additional testing results or other comparable evidence for review is necessary to demonstrate qualification of this hardware component. The NRC staff review of the scope of the HFC qualification program is discussed in Section 3.3.1 of this SE.

3. The qualification testing for the HFC-6000 platform does not establish qualification of the HFC-AI16F module under the environmental stress or EMI/RFI conditions defined in EPRI TR-107330. Submission of additional testing results or other comparable evidence for review is necessary to demonstrate qualification of this hardware component. The NRC staff review of the establishment of a baseline performance envelope under the HFC qualification program is discussed in Section 3.3.2 of this SE.

4. The qualification testing for the HFC-6000 platform does not establish qualification of analog response time performance when the platform is subjected to the environmental extremes of the generic service conditions defined in EPRI TR-107330. Submission of additional testing results or other comparable evidence for review is necessary to demonstrate qualification of the analog

response time for the HFC-6000 platform as part of a comprehensive, credible qualified performance envelope. The NRC staff review of the establishment of a baseline performance envelope under the HFC qualification program is discussed in Section 3.3.2 of this SE.

5. The qualification testing for the HFC-6000 platform does not demonstrate an environmental stress withstand capability for several key performance characteristics that are necessary to establish suitability of the platform for use in safety-related applications. Submission of additional testing results or other comparable evidence for review is necessary to demonstrate qualification of the HFC-6000 platform under the environmental stress conditions defined in EPRI-TR-107330. The NRC staff review of environmental stress withstand testing under the HFC qualification program is discussed in Section 3.3.3 of this SE.

Combine these items.

6. The qualification testing for the HFC-6000 platform does not demonstrate EMC qualification for radiated electric field emissions from 10 kHz to 10 GHz. Submission of additional testing results or other comparable evidence for review is necessary to demonstrate acceptable control of high frequency radiated emissions and establish EMC qualification of the HFC-6000 platform for radiated electric field emissions. The NRC staff review of EM emissions testing under the HFC qualification program is discussed in Section 3.3.5.1 of this SE.

7. The qualification testing for the HFC-6000 platform does not demonstrate EMC qualification for radiated electric field (high frequency) interference, high frequency conducted interference, and low frequency conducted interference. Submission of additional testing results or other comparable evidence for review is necessary to demonstrate EMC qualification for immunity to radiated electric fields, low frequency conducted interference, and high frequency conducted interference. The NRC staff review of EMI/RFI susceptibility testing under the HFC qualification program is discussed in Section 3.3.5.2 of this SE.

8. The qualification testing for the HFC-6000 platform does not demonstrate EMC qualification for radiated susceptibility over the frequency range from 1 GHz to 10 GHz and conducted susceptibility of signal leads. Submission of additional testing results or other comparable evidence for review is necessary to demonstrate EMC qualification for immunity of signal lines to low frequency conducted interference and high frequency conducted interference and platform immunity to very high frequency radiated electric field interference. The NRC staff review of EMI/RFI susceptibility testing under the HFC qualification program is discussed in Section 3.3.5.2 of this SE.

5.2 Plant-Specific Action Items

The following plant-specific actions must be performed by an applicant when requesting NRC approval for installation of a safety-related system based on the HFC-6000 platform.

1. The licensee must establish full compliance with the design criteria and regulations identified in SRP Chapter 7, Table 7.1, that are relevant to the

specific application(s) of the HFC-6000 platform as a safety-related digital I&C system in a nuclear power plant (see Section 2.2 of this SE).

2. If this SE is referenced in plant licensing documentation, the licensee must demonstrate that the HFC-6000 platform used to implement the plant-specific system is unchanged from the base platform addressed in this SE. Otherwise, the licensee must clearly and completely identify any modification or addition to the base HFC-6000 platform as it is employed and provide evidence of compliance by the modified platform with all applicable regulations that are affected by the changes (see Section 2.1 of this SE).

Combine these items.

3. The licensee must demonstrate that execution of the HFC software QA program, with its constituent life cycle processes, plans, and procedures, for the planning, design, implementation, testing, and installation of application software, along with the introduction of any new functionality within the operating software (i.e., new software), complies with the regulatory requirements of Appendix B to 10 CFR Part 50 and is equivalent to industry standards and practices endorsed by the NRC, as referenced in SRP BTP 7-14 (see Section 2.1 of this SE).

4. For a specific safety-related system project, the licensee is responsible for assuring that life cycle planning documentation for new software (e.g., application software) development under the HFC software QA program complies with the regulatory requirements of Appendix B to 10 CFR 50 and satisfies equivalent guidance to that provided by industry standards and practices endorsed by the NRC, as referenced in SRP BTP 7-14 (see Section 3.2.2 of this SE).

5. For an specific application, a software installation plan must be generated that addresses the criteria in BTP 7-14, Section B.3.1.5 (see Section 3.2.2.5 of this SE).

6. The licensee must confirm that all firmware versions installed in HFC-6000 modules are directly validated at the HFC facility prior to shipment for site acceptance and installation at the nuclear power plant (see Section 3.2.2.11 of this SE).

7. The licensee must confirm that the qualification envelope for the HFC-6000 platform complies with the generic qualification requirements specified in EPRI TR-107330 and either EPRI TR-102323, Revision 1, or RG 1.180, Revision 1 (see Sections 3.3 and 5.1 of this SE).

Otherwise, the licensee must demonstrate the application using HFC-6000 platform qualifies plant-specific safety conditions.

8. The licensee must demonstrate that the generic qualification envelope for the HFC-6000 platform bounds the corresponding plant-specific conditions (i.e., temperature, humidity, seismic, and EMC) for the location(s) in which the equipment is to be installed and that the performance characteristics demonstrated for the HFC-6000 platform under the tested service conditions are adequate for the specific application (see Sections 3.3, 3.8.2.4, and 3.8.2.6.2 of this SE).

9. The licensee must demonstrate that the generically qualified radiation withstand capability of the HFC-6000 platform bounds the expected radiation exposure for

the location(s) in which the equipment is to be installed (see Section 3.3.4 of this SE).

10. The licensee must confirm that HFC-6000 equipment is not installed in close proximity to CRTs, motors, high-current cabling or other strong radiated magnetic field emitters. Otherwise, the licensee must demonstrate adequate immunity of the HFC-6000 platform to radiated magnetic field interference (see Section 3.3.5.2 of this SE).

11. The licensee must demonstrate that that generically qualified surge withstand capability of the HFC-6000 platform bounds the expected electrical surge environment for the location(s) in which the equipment is to be installed (see Section 3.3.5.3 of this SE).

12. The licensee must confirm that fiber optic cabling is employed for the safety C-Link network and the fiber optic coupling between the HFC-SBC06 modules and the physical medium of the C-Link provides adequate electrical isolation (see Sections 3.3.5.5 and 3.8.2.6 of this SE).

13. If a specific application requires Class 1E to non-Class 1E isolation to be provided by those qualified HFC-6000 IOMs, then the licensee must demonstrate that the generic qualification envelope for the specific module(s) employed to provide electrical isolation bounds the maximum credible voltages applied to the interconnected non-Class 1E equipment. Furthermore, the licensee must demonstrate that the execution of the safety function implemented using the HFC-6000 platform will be unaffected by loss of the I/O capability of any of those modules due to damage while providing electrical isolation (see Section 3.3.5.5 of this SE).

14. The licensee must demonstrate that the qualified seismic withstand capability of the HFC-6000 platform bounds the plant-specific seismic withstand requirements (see Section 3.3.6 of this SE).

15. The licensee must confirm that locking bars are installed for the power supply assemblies in the PSM rack of the HFC-6000 platform to ensure the qualified seismic withstand capability is not compromised (see Section 3.3.6 of this SE).

16. The licensee must provide two independent AC power sources to separately supply the redundant PSM groups within the HFC-6000 power supply rack to ensure that adequate hold up time is provided for power interruption conditions (see Sections 3.3.2 and 3.8.5 of this SE).

17. The licensee must establish the suitability of the response time characteristics of the HFC-6000 platform for any particular application. In effect, the capability of the HFC-6000 platform to satisfy application-specific requirements for system response time must be demonstrated on a plant-specific basis in terms of the accident analyses in Chapter 15 of the safety analysis report of the plant (see Sections 3.3.2 and 3.8.2.5 of this SE).

18. Since the response time performance baseline for the HFC-6000 qualification program is limited to the AI16F analog input module in combination with the DO8J digital output module and the DI16I digital input in combination with the DO8J digital output module, the licensee must demonstrate acceptable response time for other input-output combinations as warranted by the plant-specific system design (see Sections 3.3.2 and 3.8.2.5 of this SE).

19. The licensee must demonstrate that the response time performance of a safety-related system based on the HFC-6000 platform satisfies application-specific requirements established in Chapter 15 of the safety analysis report for the plant. In particular, the licensee must perform timing analyses and functional testing for a particular application implementation and system configuration to demonstrate acceptability for satisfying regulatory requirements (see Section 3.4.1 of this SE).

20. The licensee must demonstrate that the cycle time allocated to the application program, and consequential processor loading, permits execution of the safety function at least once in the available task execution cycle and is consistent with the plant-specific response time requirements (see Section 3.4.2 of this SE).

21. The licensee must confirm that no UCP messaging is employed for online, in-service use other than the inter-processor communication that has been evaluated. Furthermore, the licensee must confirm that adherence to the design principle that prohibits peer-to-peer communication on the C-Link safety network (see Sections 3.4.2 and 3.5.2.1 of this SE).

22. The licensee must demonstrate that any device (e.g., gateway to other systems or networks) installed as a node on the C-Link safety network provides strictly unidirectional communication (i.e., receive only) and fulfills electrical, physical, and communications independence and security requirements (see Sections 3.5.1.2, 3.5.2.1, 3.6.3.2, 3.8.2.6.3.1, and 3.9.1.4 of this SE).

23. The licensee must ensure that full inspection of each HFC-6000 module is conducted to verify that the correct, unmodified version of the HFC-6000 operating software is installed in firmware (see Section 3.6.3.2 of this SE).

24. The licensee must establish usage procedures for the HFC-6000 platform regarding service and maintenance of the plant-specific implementation. In particular, the procedures must address limitation of software maintenance activities to offline, out-of-service conditions, including specifying configuration options for write protect control regarding initial equalization and runtime protection of application software (i.e., the preferred switch setting during controller initialization and normal operation) and controller boot up regarding power-up/reset validation of the application software (i.e., jumper settings to enable comparison of Flash memory against PROM for the application executable). Any claims related to the security features affected by these configuration setting options must be confirmed (see Section 3.6.4 of this SE).

25. The licensee must ensure that an application-specific FMEA addresses the effects of hardware CCF (see 3.8.2.15 of this SE).

26. Since the FMEA for the HFC-6000 platform identified failures that can be detected only by surveillance, software diagnostics and automatic self-tests have not been demonstrated to provide comprehensive coverage of all platform failures nor are they sufficient in and of themselves to eliminate the need for periodic surveillance testing. Consequently, the licensee must establish the additional periodic surveillance testing that is necessary to detect system failures for which automatic detection is not provided and define appropriate surveillance intervals to provide acceptable comprehensive coverage of identifiable system failure modes (see Sections 3.8.2.1, 3.8.2.5, and 3.8.2.7 of this SE).

27. The licensee must demonstrate that any plant-specific claims regarding quantification of reliability and availability address the impact of surveillance intervals on mean time to repair as part of the analysis. Furthermore, the licensee must demonstrate that any reliability and availability analysis addresses the impact of hardware CCF on availability (see Section 3.8.2.15 of this SE).

28. The licensee must perform a plant-specific D3 analysis for safety-related applications of the HFC-6000 platform (see Section 3.7 of this SE).

29. The licensee must determine those physical configuration and plant-specific installation conditions that impact safety system maintenance and define any necessary diagnostic, testing, or surveillance functions to be implemented in application software to support maintenance and repair (see Section 3.8.2.10 of this SE).

30. Since the TR for the HFC-6000 platform does not comprehensively document uncertainty calculation parameter values (e.g., hysteresis, drift) associated with the platform, the licensee must perform an analysis of accuracy, repeatability, thermal effects and other necessary data for use in determining the contribution of the HFC-6000 platform to instrumentation uncertainty in support of setpoint calculations (see Section 3.8.3 of this SE).

6.0 CONCLUSION

Based on the findings of Section 3.0 that are summarized in Section 4.0 of this SE, the NRC staff concludes that, when properly installed and used, the HFC-6000 platform is acceptable for safety-related use in nuclear power plants, subject to satisfactory licensee compliance with the Limitations and Conditions identified in Section 5.0 of this SE.

7.0 REFERENCES

1. HF Controls Corp. letter to NRC, "Doosan-HF Controls and Doosan Heavy Industries & Construction Submittal of Topical Report for Safety Evaluation," March 5, 2008 (Agencywide Documents and Management System (ADAMS) Accession No. ML080780169).

2. HF Controls Corp. letter to NRC, "Doosan-HF Controls and Doosan Heavy Industries & Construction Submittal of Topical Report for Safety Evaluation," November 15, 2007 (ADAMS Accession No. ML073390048).

3. HF Controls Corp. letter to NRC, "Acceptance for Review of HF Controls Corporation's Topical Report, PP901-000-01, Revision C, 'HFC-6000 Safety System' (TAC MD8462)," January 16, 2009 (ADAMS Accession No. ML090710918).

4. HF Controls Corp. letter to NRC, "Supporting Documents for HF Controls Corporation Topical Report, PP901-000-01, Revision C, 'HFC-6000 Safety System' (TAC MD8462)," May 29, 2009 (ADAMS Accession No. ML091540435).

5. HF Controls Corp. letter to NRC, "Supporting Documents for HF Controls Corporation Topical Report, PP901-000-01, Revision C, 'HFC-6000 Safety System' (TAC MD8462); Revised Technical Documents," June 12, 2009 (ADAMS Accession No. ML091700305).

6. HF Controls Corp. letter to NRC, "Documents as Responses to Conference Call with NRC on 7-9-09 1:00PM – 2:30PM EST with Regard to Topical Report, PP901-000-01, Revision C, 'HFC-6000 Safety System'," July 20, 2009 (ADAMS Accession No. ML092020394).

7. HF Controls Corp. letter to NRC, "Responses to RAI Part 3 for HFC-6000 Safety Control System Topical Report PP901-000-01 Revision C (TAC NO. MD8462)," February 19, 2010 (ADAMS Accession No. ML101110259).

8. HF Controls Corp. letter to NRC, "Supplementary Documents for Responses to RAI Part 3 for HFC-6000 Safety Control System Topical Report PP901-000-01 Revision C (TAC NO. MD8462)," March 12, 2010 (ADAMS Accession No. ML100780218).

9. HF Controls Corp. letter to NRC, "Revision to Responses to RAI Part 3 for HFC-6000 Safety Control (TAC NO. MD8462)," March 19, 2010 (ADAMS Accession No. ML100820252).

10. HF Controls Corp. letter to NRC, "Supporting Documents for HFC-6000 Safety Control System Safety Evaluation Report," May 6, 2010 (ADAMS Accession No. ML101320414).

11. HF Controls Corp. letter to NRC, "Supporting Documents for HFC-6000 Safety Evaluation Report Final Qualification Closure," June 18, 2010 (ADAMS Accession No. ML101790205).

12. Doosan HF Controls, "HFC-6000 Safety System Topical Report," PP901-000-01, Revision C, March 13, 2008 (ADAMS Accession No. ML080780170, pp. 2 -162).

13. NRC letter to HF Controls Corp., "Acceptance for Review of HF Controls Corporation's Topical Report, PP901-000-01, Revision C, 'HFC-6000 Safety System' (TAC MD8462)," September 16, 2008 (ADAMS Accession No. ML082460632).

14. Enclosure 1 from HF Controls Corp. letter to NRC, "HFC-6000 Topical Report Additional Information Requested by the NRC September 16, 2008," January 16, 2009 (ADAMS Accession No. ML090710921).

15. Enclosure 1 from NRC letter to HF Controls Corp., "Audit Report for the Audit of the HFC-6000 Platform at Doosan HF Controls on October 6-9, 2009," January 27, 2010 (ADAMS Accession No. ML093580045).

16. Enclosure 2 from NRC letter to HF Controls Corp., "Report for the Audit of the HFC-6000 Platform at Doosan HF Controls on December 16-18, 2009," April 14, 2010 (ADAMS Accession No. ML100900441).

17. Doosan HF Controls, "Responses to RAI Part 3 from NRC in correspondence to Topical Report PP901-000-01 Revision C," RR901-001-01, Revision A, February 19, 2010 (ADAMS Accession No. ML101110260).

18. Doosan HF Controls, "Revision to Responses to NRC RAI Part 3," RR901-001-02, Revision A, March 19, 2010 (ADAMS Accession No. ML100820253).

19. Doosan HF Controls, "HFC-6000 Product Line Requirements Specification," RS901-000-01, Revision F, July 14, 2009 (ADAMS Accession No. ML092020402, pp. 17-29).

20. Doosan HF Controls, "HFC-6000 Product Line Document Map," PP901-000-02, Revision A, November 17, 2004 (ADAMS Accession No. ML073600035, pp. 291-298).

21. Doosan HF Controls, "Control Systems C-Link Protocol Software Component Design Specification," DS002-000-01, Revision C, May 15, 2007 (ADAMS Accession No. ML083450133, pp. 336-366).

22. Doosan HF Controls, "Universal Communications Protocol Component Design Specification," DS002-000-03, Revision B, February 16, 2006 (ADAMS Accession No. ML083450133, pp. 367-387).

23. NRC letter to Siemens Power Company, "Acceptance for Referencing of Licensing Topical Report EMF-2110(NP), Revision 1, 'Teleperm XS: A Digital Reactor Protection System' (TAC No. MA1983)," May 5, 2000 (ADAMS Accession No. ML003711856).

24. NRC letter to Westinghouse Electric Company, "Acceptance for Referencing of Topical Report CENPD-396-P, Revision 01, 'Common Qualified Platform,' and Appendices 1, 2, 3, and 4, Revision 01 (TAC No. MA1677)," August 11, 2000 (ADAMS Accession No. ML003740165).

25. NRC letter to Triconex Corporation, "Review Of Triconex Corporation Topical Reports 7286-545, 'Qualification Summary Report' and 7286-546, 'Amendment 1 To Qualification Summary Report,' Revision 1 (TAC No. MA8283)," December 11, 2001 (ADAMS Accession No. ML013470433).

26. NRC letter to Wolf Creek Nuclear Operating Corporation, "Wolf Creek Generating Station – Issuance of Amendment RE: Modification of the Main Steam and Feedwater Isolation System Controls (TAC No. MD4839)," March 31, 2009 (ADAMS Accession No. ML090610317).

27. NRC letter to Duke Energy Carolinas, LLC, "Oconee Nuclear Station, Units 1, 2, and 3, Issuance of Amendments Regarding Acceptance of the Reactor Protective System and Engineered Safeguard Protective System (RPS/ESPS) Digital Upgrade (TAC Nos. MD7999, MD8000, AND MD8001)," January 28, 2010 (ADAMS Accession No. ML100220016).

28. Doosan HF Controls, "HFC-6000 Safety Control System Security Concept," RR901-000-23, Revision A, November 19, 2009 (ADAMS Accession No. ML101110264).

29. Doosan HF Controls, "19 Inch Rack Power Supply Requirements Specification," RS901-000-12, Revision A, January 4, 2005 (ADAMS Accession No. ML100780220).

30. Doosan HF Controls, "HFC-SBC06-DPM06 Boards Module Design Specification System Controller," MS901-000-01, Revision E, March 27, 2009 (ADAMS Accession No. ML091700304, pp. 1-55).

31. Doosan HF Controls, "HFC-SBC06-DPM06 Module Detailed Design Specification," DS901-000-01, Revision D, December 12, 2008 (ADAMS Accession No. ML091700304, pp. 79-117).

32. Doosan HF Controls, "RAI #2 Response of Revision A TR Review (MC5380)," March 13, 2008 (ADAMS Accession No. ML080780170, pp. 163-196).

33. Doosan HF Controls, "HFC-6000 I/O Card Module Design Specification," MS901-000-02, Revision C, January 29, 2009 (ADAMS Accession No. ML091700304, pp. 56-78).

34. Doosan HF Controls, "HFC-6000 I/O Board Module Detailed Design Specification," DS901-000-02, Revision A, November 18, 2003 (ADAMS Accession No. ML073600035, pp. 88-96).

35. Doosan HF Controls, "HFC-DI16I Board Module Detailed Design Specification, Sixteen Channel Digital Input Board," DS901-000-04, Revision B, May 7, 2007 (ADAMS Accession No. ML073600035, pp. 105-119).

36. Doosan HF Controls, "HFC-DO8J Board Module Detailed Design Specification, Eight Channel Relay Digital Output Board," DS901-000-03, Revision B, January 30, 2009 (ADAMS Accession No. ML091700304, pp. 108-116).

37. Doosan HF Controls, "HFC-DC33 Board Module Detailed Design Specification, Digital Input/Output Controller Board Specific for Motor Operated Valve (MOV)," DS901-000-05, Revision D, November 30, 2007 (ADAMS Accession No. ML091700304, pp. 117-130).

38. Doosan HF Controls, “HFC-DC34 Board Module Detailed Design Specification, Digital Input/Output Controller Board Specific for Electronically Operated Breakers (EOB),” DS901-000-06, Revision D, November 30, 2007 (ADAMS Accession No. ML091700304, pp. 131-143).

39. Doosan HF Controls, “HFC-AI4K Module Detailed Design Specification, Pulse Input Board,” DS901-000-12, Revision B, February 4, 2009 (ADAMS Accession No. ML091700304, pp. 173-191).

40. Doosan HF Controls, “HFC-AI16 Board Detailed Design Specification, Sixteen Channel Analog Input Board,” DS901-000-07, Revision D, February 2, 2009 (ADAMS Accession No. ML091700304, pp. 144-160).

41. Doosan HF Controls, “HFC-AO8 Board Module Detailed Design Specification, Eight Channel Analog Output Board,” DS901-000-08, Revision D, February 2, 2009 (ADAMS Accession No. ML091700304, pp. 161-172).

42. Doosan HF Controls, “HFC-AI8M Module Detailed Design Specification, Eight Channel RTD Input Board,” DS901-000-11, Revision B, March 12, 2007 (ADAMS Accession No. ML073600035, pp. 173-195).

43. Doosan HF Controls, “HFC-SBC06 and HFC-DPM06 CPLD Design Specification,” DS901-000-75, Revision C, December 10, 2009 (ADAMS Accession No. ML100820253, pp 25-38).

44. Doosan HF Controls, “Component Design Specification Operating System,” DS001-000-01, Revision B, May 15, 2007 (ADAMS Accession No. ML073600035, pp. 21-48).

45. Doosan HF Controls, “Component Design Specification HFC-Controller Equation Interpreter,” DS001-000-02, Draft A, February 16, 2005 (ADAMS Accession No. ML083450133, pp. 239-335).

46. Doosan HF Controls, “HFC Control System Components, CQ4 Blocks, General Information For CQ4 Blocks,” DS001-000-03, Revision A, March 15, 2005 (ADAMS Accession No. ML083450133, pp. 64-77).

47. Doosan HF Controls, “Design Specification System Software Components,” DS001-000-06, Revision A, March 10, 2005 (ADAMS Accession No. ML083450133, pp. 388-421).

48. Doosan HF Controls, “Redundancy and Failover Mechanism Component Design Specification,” DS001-000-08, Revision C, May 15, 2007 (ADAMS Accession No. ML083450133, pp. 77-99).

49. Doosan HF Controls, “HFC Control Systems ICL Protocol Component Design Specification Inter-Communications Link,” DS002-000-02, Revision D, May 15, 2007 (ADAMS Accession No. ML083450133, pp. 100-120).

50. Doosan HF Controls, "HFC-6000 Software Configuration for Nuclear Safety Equipment Controller," DS001-000-07, Revision B, January 14, 2010 (ADAMS Accession No. ML101110262).

51. Doosan HF Controls, "HFControls Control System, One-Step Software User's Guide, Software Revision 2.50," UG04-000-04, Revision C, September 4, 2007 (ADAMS Accession No. ML083450133, pp. 422-499).

52. Doosan HF Controls, "Commercial Grade Software Evaluation," QPP 7.3, Revision C, October 22, 2007 (ADAMS Accession No. ML092020394, pp. 32-59).

53. Doosan HF Controls, "HFC-SBC06 Main Processor System Firmware," CGSE002, Revision A, December 15, 2005 (ADAMS Accession No. ML090830343).

54. Doosan HF Controls, "HFC-SBC06 SAP System Firmware," CGSE003 Revision A, December 15, 2005 (ADAMS Accession No. ML090830344).

55. Doosan HF Controls, "HFC-SB06 SEP System Firmware," CGSE004 Revision A, December 15, 2005 (ADAMS Accession No. ML090830345).

56. Doosan HF Controls, "HFC-AI16F Firmware," CGSE005 Revision A, December 15, 2005 (ADAMS Accession No. ML090830346).

57. Doosan HF Controls, "HFC-A14K Firmware," CGSE006 Revision A, December 15, 2005 (ADAMS Accession No. ML090830347).

58. Doosan HF Controls, "HFC-AI8M Firmware," CGSE007 Revision A, December 15, 2005 (ADAMS Accession No. ML090830348).

59. Doosan HF Controls, "HFC-AO8F Firmware," CGSE008 Revision A, December 15, 2005 (ADAMS Accession No. ML090830349).

60. Doosan HF Controls, "HFC-DC33 Firmware," CGSE009 Revision A, December 15, 2005 (ADAMS Accession No. ML090830351).

61. Doosan HF Controls, "HFC-DC34 Firmware," CGSE010 Revision A, December 15, 2005 (ADAMS Accession No. ML090830352).

62. Doosan HF Controls, "HFC-DI16I Firmware," CGSE011 Revision A, December 15, 2005 (ADAMS Accession No. ML090830353).

63. Doosan HF Controls, "HFC-DO8J Firmware," CGSE012 Revision A, December 15, 2005 (ADAMS Accession No. ML090830354).

64. Doosan HF Controls, "Source Code Review," WI-ENG-830, Revision A, August 2, 2004 (ADAMS Accession No. ML090710921, pp. 53-58).

65. Doosan HF Controls, "Code Review Record," 909008, Revision 1, September 19, 2008 (ADAMS Accession No. ML090710921, pp. 36-51).

66. Doosan HF Controls, "Verification and Validation Report," VV0415, Revision A, December 7, 2005 (ADAMS Accession No. ML090830340).

67. Doosan HF Controls, "Condition Report," CR No. 2009-0626, May 5, 2010 (ADAMS Accession No. ML101320416).

68. Doosan HF Controls, "Application Software Objects Test Report," TR001-000-02, Revision B, December 10, 2009 (ADAMS Accession No. ML101790205, pp. 176-188).

69. Doosan HF Controls, "Component Test Procedure," TS001-000-01, Revision A, October 28, 2004 (ADAMS Accession No. ML092020402, pp. 30-39).

70. Doosan HF Controls, "Condition Report," CR No. 2009-0631, February 1, 2010 (ADAMS Accession No. ML100820253, pp. 22-24).

71. Doosan HF Controls, "Additional OS Testing," TS901-001-23, Revision A, June 11, 2010 (ADAMS Accession No. ML101790205, pp. 189-199).

72. Doosan HF Controls, "HFC-SBC06/DPM06 Prototype Test Procedure," TS901-000-02, Revision B, September 22, 2004 (ADAMS Accession No. ML092020402, pp. 40-59).

73. Doosan HF Controls, "HFC-DC33 Prototype Test Procedure," TS901-000-09, Revision D, November 27, 2007 (ADAMS Accession No. ML092020402, pp. 60-84).

74. Doosan HF Controls, "HFC-DO8J Prototype Test Procedure," TS901-000-12, Revision B, September 22, 2004 (ADAMS Accession No. ML092020403, pp. 1-19).

75. Doosan HF Controls, "HFC-6000 Digital and Analog Board Functional Test," 400484-03, Revision F, April 13, 2009 (ADAMS Accession No. ML092020403, pp. 51-83).

76. Doosan HF Controls, "HFC-6000 Control System, ERD111 – Control System Qualification Project, Operability Test Procedure," TP0402, Revision F, January 3, 2005 (ADAMS Accession No. ML073600054, pp. 240-255).

77. Doosan HF Controls, "HFC-6000 Control System, ERD111 – Control System Qualification Project, Prudency Test Procedure," TP0403, Revision F, January 3, 2005 (ADAMS Accession No. ML073600054, pp. 324-351).

78. Doosan HF Controls, "Condition Report," CR No. 2009-0625, February 2, 2010 (ADAMS Accession No. ML100820253, pp. 16-18).

79. Doosan HF Controls, "Addendum to TP0402 Revision F," TN901-000-09, Revision B, December 29, 2009 (ADAMS Accession No. ML100780219).

80. Doosan HF Controls, "HFC QA Program Manual," QAPM, Revision G, November 8, 2007 (ADAMS Accession No. ML073390064, pp. 626-659).

81. Doosan HF Controls, "Organizational Responsibilities," QPP 1.2, Revision C, November 8, 2007 (ADAMS Accession No. ML073600035, pp. 355-366).

82. Doosan HF Controls, "Project Quality Plans," QPP 2.1, Revision E, May 12, 2009 (ADAMS Accession No. ML091540436, pp. 194-202).

83. Doosan HF Controls, "Software Security," WI-ENG-020, Revision B, September 22, 2009 (ADAMS Accession No. ML101110266).

84. Doosan HF Controls, "HFC-6000 Software Safety Plan," PP004-000-01, Revision C, July 14, 2009 (ADAMS Accession No. ML092020394, pp. 7-31).

85. Doosan HF Controls, "Product Development Plan," VV0401, Revision B, November 8, 2007 (ADAMS Accession No. ML073390064, pp. 91-121).

86. Doosan HF Controls, "Project Quality Plan," PQP 2003-05, Revision D, November 8, 2007 (ADAMS Accession No. ML073600035, pp. 299-314).

87. Doosan HF Controls, "Software Lifecycle and Verification/Validation Program," QPP 3.2, Revision F, November 20, 2007 (ADAMS Accession No. ML073600054, pp. 14-39).

88. Doosan HF Controls, "Software Verification and Validation," WI-ENG-022, Revision F, November 20, 2007 (ADAMS Accession No. ML090830342).

89. Doosan HF Controls, "Corrective Action Program," QPP 16.1, Revision H, June 13, 2007 (ADAMS Accession No. ML073600054, pp. 40-51).

90. Doosan HF Controls, "Configuration Management," WI-ENG-003, Rev D, January 11, 2007 (ADAMS Accession No. ML090830341).

91. Doosan HF Controls, "10 CFR Part 21 Reporting," QPP 16.3, Revision 0, July 26, 2001 (ADAMS Accession No. ML073600054, pp. 52-57).

92. Doosan HF Controls, "HFC-6000 Control System, ERD111 – Control System Qualification Project, Baseline Testing Summary Report," TS901-000-22, Revision B, October 16, 2007 (ADAMS Accession No. ML073600062, pp. 87-183).

93. Doosan HF Controls, "ERD111 Performance Envelope," RR901-000-37, Revision B, December 16, 2009 (ADAMS Accession No. ML100780221).

94. Doosan HF Controls, "HFC-6000 Controller SC, SAP, SEP Firmware Requirements Specification," RS901-000-37, Revision A, May 15, 2007 (ADAMS Accession No. ML090710921, pp. 565-580).

95. Doosan HF Controls, "General I/O Cards Requirements Specification," 700901-06, Revision F, August 8, 2007 (ADAMS Accession No. ML092020403, pp. 95-123).

96. Doosan HF Controls, "Design Control Process," QPP 3.1, Revision F, June 13, 2007 (ADAMS Accession No. ML073600054, pp. 1-13).

97. Doosan HF Controls, "HFC-6000 Product Line (Pre-Developed Software – PDS) Traceability Matrix," RR901-000-31, Revision H, June 16, 2010 (ADAMS Accession No. ML101790205, pp 49-67).

98. Doosan HF Controls, "CQ4 Requirement Traceability Matrix," RR901-000-31, Attachment A, Revision A, December 2, 2009 (ADAMS Accession No. ML100780334).

99. Doosan HF Controls, "Equation Interpreter Requirement Traceability Matrix," RR901-000-31, Attachment B, Revision B, January 13, 2010 (ADAMS Accession No. ML100780335).

100 Doosan HF Controls, "I/O Card Requirement Traceability Matrix," RR901-000-31, Attachment C, Revision A, December 10, 2009 (ADAMS Accession No. ML100780336).

101. Doosan HF Controls, "Condition Report," CR No. 2009-0539, November 23, 2009 (ADAMS Accession No. ML101110267, pp. 24-26).

102. Doosan HF Controls, "Condition Report," CR No. 2009-0623, January 25, 2010 (ADAMS Accession No. ML100820253, pp. 10-12).

103. Doosan HF Controls, "HFC-6000 Controller and HFC-DPM06 SC, SAP, SEP Firmware, VHDL Program Code Requirements Specification," RS901-000-37, Revision I, June 6, 2010 (ADAMS Accession No. ML100780222).

104. Doosan HF Controls, "HFC Control System Components, CQ4 Blocks, Common Requirements for CQ4 Blocks," RS901-000-37, Appendix A, Revision B, November 24, 2009 (ADAMS Accession No. ML100780223).

105. Doosan HF Controls, "HFC Control System Components, Equation Interpreter, Equation Common Requirements," RS901-000-37, Appendix B, Revision D, January 7, 2010 (ADAMS Accession No. ML100780224).

106. HF Controls Corp. letter to NRC, "Summary of June 15, 2010 conference call and HFC commitment for final qualification closure retesting," June 16, 2010 (ADAMS Accession No. ML101680379).

107. Doosan HF Controls, "HFC-6000 Control System, ERD111 – Control System Qualification Project, Master Test Plan," TN0401, Revision C, January 19, 2004 (ADAMS Accession No. ML073390049, pp. 150-198).

108. Doosan HF Controls, "HFC-6000 Control System, Safety-Related Control System Qualification, Test Specimen Design Description," DD0401, Revision A, April 9, 2003 (ADAMS Accession No. ML073390064, pp. 69-90).

109. Doosan HF Controls, "HFC-6000 Product Line Components, TSAP Requirements Specification," 700901-09, Revision A, August 7, 2003 (ADAMS Accession No. ML083450133, pp. 2-13).

110. Doosan HF Controls, "HFC-6000 Control System, TSAP Design Specification," ADS0401, Revision A, September 11, 2003 (ADAMS Accession No. ML083450133, pp. 137-157).

111. Doosan HF Controls, "HFC-6000 Control System, ERD111 – Control System Qualification Project, Integration (Setup and Checkout) Procedure," TP0401, Revision A, January 30, 2004 (ADAMS Accession No. ML073390049, pp. 199-215).

112. Doosan HF Controls, "HFC-6000 Control System, ERD111 – Control System Qualification Project, Environmental Stress Test Procedure," TP0404, Revision C, January 23, 2004 (ADAMS Accession No. ML073390049, pp. 416-436).

113. Doosan HF Controls, "HFC-6000 Control System, ERD111 – Control System Qualification Project, Seismic Test Procedure," TP0405, Revision D, August 16, 2004 (ADAMS Accession No. ML073390049, pp. 437-458).

114. Doosan HF Controls, "HFC-6000 Control System, ERD111 – Control System Qualification Project, Surge Withstand Test Procedure," TP0406, Revision C, January 23, 2004 (ADAMS Accession No. ML073390055, pp. 103-130).

115. Doosan HF Controls, "HFC-6000 Control System, ERD111 – Control System Qualification Project, EMI/RFI Test Procedure," TP0407, Revision C, January 23, 2004 (ADAMS Accession No. ML073390055, pp. 131-155).

116. Doosan HF Controls, "HFC-6000 Control System, ERD111 – Control System Qualification Project, TSAP Validation Test Procedure," TP0408, Revision B, January 3, 2005 (ADAMS Accession No. ML073600054, pp. 449-504).

117. Doosan HF Controls, "HFC-6000 Control System, ERD111 – Control System Qualification Project, Test Specimen Validation Test Procedure," TP0408B, Revision B, September 23, 2004 (ADAMS Accession No. ML073600062, pp. 1-16).

118. Doosan HF Controls, "HFC-6000 Control System, ERD111 – Control System Qualification Project, ESD Test Procedure," TP0409, Revision C, January 23, 2004 (ADAMS Accession No. ML073600062, pp. 17-39).

119. Doosan HF Controls, "HFC-6000 Control System, ERD111 – Control System Qualification Project, Burn-in Test," TP0410, Revision C, January 4, 2005 (ADAMS Accession No. ML073600062, pp. 40-50).

120. Doosan HF Controls, "HFC-6000 Control System, ERD111 – Control System Qualification Project, Isolation Test Procedure," TP0411, Revision C, January 3, 2005 (ADAMS Accession No. ML073600062, pp. 51-86).

121. Doosan HF Controls, "HFC-6000 Control System, ERD111 – Control System Qualification Project, Summary Report for Burn-In Test, Setup and Checkout Test, and TSAP Validation Test," TS901-000-30, Revision B, September 15, 2007 (ADAMS Accession No. ML073600062, pp. 402-414).

122. Doosan HF Controls, "Condition Report," CR No. 2009-0624, March 16, 2010 (ADAMS Accession No. ML100820253, pp 13-15).

123. Doosan HF Controls, "HFC-6000 Control System, ERD111 – Control System Qualification Project, Post Qualification Testing Summary Report," TS901-000-29, Revision B, October 16, 2007 (ADAMS Accession No. ML073600062, pp. 375-401).

124. Doosan HF Controls, "HFC-6000 Control System, ERD111 – Control System Qualification Project, Seismic Retest In-house Testing Summary Report (Update of Pre-Qualification Tests)," TS901-000-34, Revision B, September 28, 2007 (ADAMS Accession No. ML073600062, pp. 415-466).

125. Doosan HF Controls, "Condition Report," CR No. 2009-0630, April 30, 2010 (ADAMS Accession No. ML101320416, pp. 9-11).

126. Doosan HF Controls, "HFC-6000 Control System, ERD111 – Control System Qualification Project, Environmental Testing Summary Report," TS901-000-23, Revision B, September 26, 2007 (ADAMS Accession No. ML073600062, pp. 184-279).

127. Doosan HF Controls, "Addendum to TS901-000-34 Rev B, Seismic Retest In-house Testing Summary Report," TN901-000-07, Revision A, December 9, 2009 (ADAMS Accession No. ML101790206, pp. 84-93).

128. Doosan HF Controls, "Condition Report," CR No. 2009-0543, December 15, 2009 (ADAMS Accession No. ML).

129. Doosan HF Controls, "HFC-6000 Qualification System vs. EPRI TR 107330 Operating Envelope," RR901-000-41, Revision A, February 19, 2010 (ADAMS Accession No. ML101110267).

130. Doosan HF Controls, "HFC-6000 Product Line, Addendum to TS901-000-23 Rev C, Environmental Test Summary Report," TN901-000-05, Revision A, December 9, 2009 (ADAMS Accession No. ML101790206, pp. 43-65).

131. Doosan HF Controls, "HFC-6000 Product Line, Addendum to TS901-000-29 Rev B, Post Qualification Testing Report," TN901-000-06, Revision A, December 9, 2009 (ADAMS Accession No. ML101790206, pp. 66-83).

132. Doosan HF Controls, "HFC-6000 Product Line, Addendum to TS901-000-35 Revision B, Seismic Retest Summary Report," TN901-000-08, Revision A, December 9, 2009 (ADAMS Accession No. ML101790206, pp. 94-103).

133. Doosan HF Controls, "HFC-6000 Product Line, Clarifications to Qualification Test Results," TN901-000-12, Revision A, June 18, 2010 (ADAMS Accession No. ML101790205, pp. 165-175).

134. Doosan HF Controls, "HFC-6000 Radiation Exposure Evaluation," RR901-000-36, Revision A, November 12, 2009 (ADAMS Accession No. ML100820253, pp. 39-46).

135. Doosan HF Controls, "HFC-6000 Control System, ERD111 – Control System Qualification Project, EMI/RFI, ESD, and SWC Testing Summary Report," TS901-000-25, Revision B, September 26, 2007 (ADAMS Accession No. ML073600062, pp. 280-351).

136. Doosan HF Controls, "HFC-6000 Control System, ERD111 – Control System Qualification Project, Isolation Testing Summary Report," TS901-000-28, Revision B, September 15, 2007 (ADAMS Accession No. ML073600062, pp. 352-374).

137. Doosan HF Controls, "HFC-6000 Product Line, Nuclear Qualification Project ERD111, EPRI TR 107330 Requirements Compliance Traceability Matrix," RR901-000-10, Revision C, December 14, 2009 (ADAMS Accession No. ML101110263).

138. Doosan HF Controls, "HFC-6000 Control System, ERD111 – Control System Qualification Project, Seismic Testing Summary Report," TS901-000-35, Revision B, September 15, 2007 (ADAMS Accession No. ML073600062, pp. 467-530).

139. Doosan HF Controls, "ERD111 Seismic Qualification Analysis Report," TS901-000-44, Revision A, July 30, 2010 (ADAMS Accession No. ML102650438).

140. Doosan HF Controls, "Addendum to TP0402, Revision F," TN901-000-09, Revision B, December 29, 2009 (ADAMS Accession No. ML100780219).

141. Doosan HF Controls, "HFC-6000 Failure Modes and Effects Analysis," RR901-000-01, Revision B, April 1, 2005 (ADAMS Accession No. ML073600054, pp. 58-105).

142. Doosan HF Controls, "Security Overview," RR901-000-38, Revision A, December 14, 2009 (ADAMS Accession No. ML101110265).

143. Doosan HF Controls, "HFC-6000 Reliability and Availability Analysis Report," RR901-000-04, Revision A, November 11, 2004 (ADAMS Accession No. ML073600054, pp. 106-126).

Principle Contributors: T. Mossman
R.Wood

Date: