



HF Controls Corp. • 1624 West Crosby Road Suite 124 • Carrollton, TX 75006 USA •
Phone 469.568.6500 • Fax 469.568.6599 • www.hfcontrols.com

March 19 2008

United States Nuclear Regulatory Commission Washington, D.C.20555

Attention: Document Control Desk

Subject: Doosan-HF Controls Submittal of the Non-Proprietary HFC-6000 Topical
Report and Response to RAI#2

Reference: HFC-6000 Safety Control System

Ladies and Gentlemen:

As stated in our letter to you dated March 5, 2008, we are forwarding a copy of the Non-Proprietary version of the Topical Report Revision C and our responses to your Request for Additional Information Number 2 (RAI#2) for the HFC 6000 Safety Control System. The proprietary version of the HFC 6000 Topical Report and our responses to RAI#2 was submitted with the March 5, 2008 letter. The proprietary information for which withholding is being requested is further identified in Affidavit HFC 2008031907 signed by the owner of the proprietary information, Doosan-HF Control Cooperation. The affidavit which accompanies this letter sets forth the basis on which the information may be withheld from public disclosure by the Commission and addresses with specificity the considerations listed in paragraph (b) (4) of 10 CFR Section 2.390 of the Commission's regulations.

Doosan-HFC has employed the traditional approach for marking proprietary information by enclosing it in brackets and deleting the information from the non-proprietary version. This approach indicates without a doubt the information to be withheld from public disclosure. Each page of the proprietary version has "Proprietary" clearly stated to indicate the status of that version. This approach is in accordance with Section 2.390.

The adjacent indication of each type of proprietary material is unnecessary since the material in question consists of only one type of material, confidential commercial where its use by a competitor would improve his commercial position to the detriment of Doosan-HFC Corporation. Therefore, adjacent indication would be redundant and is considered unnecessary.

Correspondence with respect to the proprietary aspects for the application for withholding of

the Doosan-HFC affidavit should reference this letter and should be addressed to the undersigned.

Yours truly,



Allen Hsu

President
Doosan HF Controls Corp.

Enclosures:

- 1- HFC 6000 Safety Control System Topical Report -Non-Proprietary Version
- 2- Response to RAI#2-Non-Proprietary Version
- 3- Affidavit
- 4- Non-Proprietary Justification
- 5- Proprietary Information Notice

CC. Jon Thompson, NRC
Project Directorate IV-1
Mail Stop 07D1
J. Stevens, T. Gerardis Doosan HF Controls
Changho Cho, Doosan

ABSTRACT

This report describes the hardware and software technical features and provides qualification information for the HF Controls Corp. (HFC) HFC-6000 nuclear safety related instrumentation and control platform. The purpose of this report is to seek review and gain approval from the US Nuclear Regulatory Commission for the use of the HFC-6000 controller, I/O modules, communication modules and power supplies for safety related applications in US nuclear power plants. The review and approval is requested for a specified set of HFC hardware and software.

The HFC-6000 has been designed and qualified to meet the applicable safety related I&C requirements for nuclear power plants. Typical applications include:

- Reactor Protection Systems (RPS).
- Engineered Safety Features Actuation System (ESFAS) functions.
- Post Accident Monitoring Systems and Safety Parameter Display Systems.
- NSSS and Balance of Plant (BOP) safety control systems and related functions.

The HFC-6000 scalability makes it an effective approach for all nuclear power plant safety applications including small single loop controllers to complete plant control. The 19" rack mounted platform represents a modular structure whose components can be utilized for all plant safety applications. A HFC-6000 platform solution suitable for all safety applications can reduce the overall instrumentation and control complexity by minimizing operation and maintenance requirements.

The scope of this report addresses both the hardware and software associated with the HFC-6000 platform and the HFC commercial dedication process which prescribes the design and qualification techniques used to assess its reliability. Qualification of the HFC-6000 system is assessed in accordance with the guidance presented by RG 1.180 Rev 1, RG 1.209 and EPRI TR-107330. The report includes hardware and software design descriptions as well as processes by which they were designed. Hardware qualification, in addition to the verification, and validation of software quality are also included. Pre-Development Software quality was verified and validated through methods outlined in EPRI TR-106439 and IEEE Std 7-4.3.2. New software is qualified in accordance with BTP-14. Hardware was qualified through type testing in accordance with applicable regulatory guidance and the requirements of IEEE Std 323.

Regulatory concerns regarding control system defense-in-depth and diversity are summarily discussed in association with their potential respective resolutions. A detailed defense-in-depth and diversity analysis will be addressed during the plant specific licensing process. The detailed HFC 6000 system configuration, applications, and HMI will also be addressed as part of a plant specific licensing process.

The main body of this report describes the HFC-6000 controller, input/output modules, communication modules, and power suppliers with detailed discussions of the key issues cited in numerous reports and in the Standard Review Plan (NUREG-0800).

A summary of the current FMEA findings is provided in section 8. This section lists HFC-6000 potential failure modes and provides an evaluation of their probable effects.

TABLE OF CONTENTS

1	Introduction.....	1-1
1.1	Introduction to HFC.....	1-1
1.2	Introduction to HFC-6000.....	1-1
2	Documents and Definitions.....	2-1
2.1	Definitions.....	2-1
3	Acronyms.....	3-1
4	Overview of HFC-6000 Qualification Project.....	4-1
5	HFC-6000 System Overview.....	5-1
6	HFC Safety I&C Platform Hardware Description.....	6-1
6.1	System Controller Module.....	6-1
6.2	Input /Output Modules.....	6-4
6.2.1	Relay Output Module.....	6-7
6.2.2	Digital Input Module.....	6-7
6.2.3	Digital Controller Module.....	6-7
6.2.4	Digital Control of Breakers Module.....	6-7
6.2.5	Analog Input Module.....	6-8
6.2.6	Analog Output Module.....	6-8
6.2.7	RTD Input Module.....	6-8
6.2.8	Pulse Input Module.....	6-8
6.3	Communication Modules.....	6-8
6.4	Power Supplies and Chassis.....	6-10
7	HFC Safety Platform Software Description.....	7-1
7.1	Controller Software.....	7-1
7.1.1	HFC-SBC06 Controller.....	7-1
7.1.1.1	The System (SYS) Processor.....	7-3
7.1.1.2	SYS Processor Software Architecture.....	7-4
7.2	Communication Software.....	7-5
7.2.1	Communication Link (C-Link) Software.....	7-6
7.2.1.1	Message Types.....	7-6
7.2.1.2	Token Passing Scheme.....	7-6
7.2.1.3	Synchronization on Dual-Channels.....	7-7
7.2.1.4	Deterministic Nature of the C-Link.....	7-7
7.2.1.5	C-Link Processor Software Architecture.....	7-8
7.2.2	ICL Communication Software.....	7-8
7.2.2.1	I/O module communication.....	7-9
7.2.2.1.1	Redundant Serial Link.....	7-9
7.2.2.1.2	Polling Operation.....	7-9
7.2.2.1.3	Secondary Loopback Test.....	7-10
7.2.2.1.4	Secondary Polling Function.....	7-10
7.2.2.1.5	ICL Software Architecture.....	7-11
7.2.3	Input/Output Module Firmware.....	7-11
7.3	The Development and Maintenance Tools.....	7-12
8	Safety System Design Topics.....	8-1

8.1	Deterministic and Time Response	8-1
8.1.1	System Controller	8-1
8.1.2	SYS Processor Characteristics	8-1
8.1.2.1	Applications Tasks	8-2
8.1.2.2	Supervisory Tasks	8-2
8.1.3	ICL Processor Characteristics	8-2
8.1.3.1	Operation in the Primary Controller	8-2
8.1.3.2	Operation in the Secondary Controller	8-3
8.1.4	I/O Module Characteristics	8-4
8.1.5	C-Link Processor Characteristics	8-4
8.1.6	Deterministic Performance Conclusion	8-6
8.2	Failure Mode Effects Analysis (FMEA)	8-6
8.3	Reliability and Availability	8-9
8.4	Quality Assurance Programs	8-10
8.5	Regulations, Codes, Standards and Guidance for Digital System Implementation	8-13
8.5.1	General	8-13
8.5.2	Compliance with Nuclear Regulatory Commission (NRC) Documents	8-13
8.5.3	Institute of Electrical and Electronic Engineers (IEEE) Standards	8-20
8.5.4	Other Documents	8-27
8.5.5	CFR and General Design Criteria (GDC)	8-29
8.6	Defense-in-Depth and Diversity Evaluation Process	8-32
8.6.1	NRC Position 1	8-32
8.6.1.1	Compliance to Position 1	8-32
8.6.2	NRC Position 2	8-32
8.6.2.1	Compliance to Position 2	8-33
8.6.3	NRC Position 3	8-33
8.6.3.1	Compliance to Position 3	8-33
8.6.4	Critical Analog Signals	8-33
8.6.5	Critical Manual Signals	8-34
8.6.6	Implementation of Critical Manual Signals	8-34
8.6.7	Conclusion	8-34
8.7	Cyber Security	8-35
8.8	Isolation and Independence	8-36
8.9	Digital Instrumentation and Controls (DI&C) Interim Staff Guidance (ISG)-04, Communications Issues	8-37
9	Equipment Qualification	9-1
9.1	Introduction	9-1
9.2	System Qualification Test Plan	9-1
9.2.1	Scope	9-1
9.2.2	Equipment Tested	9-2
9.2.3	Safety Functions Tested	9-2
9.2.4	Test Requirements	9-3
9.2.4.1	Test Plans and Procedures	9-3
9.2.4.2	Test Sequence	9-5
9.2.4.3	Test Arrangement and Methodology	9-8

9.2.4.4	Test Personnel.....	9-9
9.2.4.5	System Operational Stress Conditions.....	9-9
9.3	System Qualification Test Results.....	9-10
9.3.1	Prequalification Tests.....	9-10
9.3.1.1	Burn-in Test (TP0410).....	9-10
9.3.1.1.1	Burn-in Test Results	9-10
9.3.1.2	System Setup and Checkout (TP0401).....	9-11
9.3.1.2.1	System Setup and Checkout Test Results.....	9-11
9.3.1.3	TSAP Validation Test Procedure (TP0408)	9-11
9.3.1.3.1	TSAP Test Results	9-12
9.3.2	Pre-Qualification Tests	9-12
9.3.2.1	Operability Tests (TP0402).....	9-12
9.3.2.1.1	Operability Test Results.....	9-13
9.3.2.1.2	Conclusion	9-14
9.3.2.2	Power Interruption Test	9-14
9.3.2.2.1	Conclusion	9-14
9.3.2.3	Prudency Tests (TP0403).....	9-15
9.3.2.3.1	Prudency BOE Test Results.....	9-15
9.3.2.3.2	Prudency Serial Port Failure Test Results	9-16
9.3.2.3.3	Prudency Serial Port Noise Test Results	9-16
9.3.3	Qualification Tests	9-17
9.3.3.1	Environmental Stress Test (TP0404).....	9-17
9.3.3.1.1	Environmental Test Results	9-18
9.3.3.2	EMI\RFI Test (TP0407).....	9-20
9.3.3.2.1	EMI/RFI Tests Results.....	9-22
9.3.3.3	ESD Test (TP0409).....	9-24
9.3.3.3.1	ESD Test Results	9-25
9.3.3.4	Surge Withstand Test (TP0406).....	9-25
9.3.3.4.1	Surge Withstand Test.....	9-25
9.3.3.4.2	Surge Withstand Test Results.....	9-26
9.3.3.5	Seismic Tests (TP0405).....	9-26
9.3.3.5.1	Seismic Test Sequence.....	9-28
9.3.3.6	Isolation Test.....	9-30
9.3.3.6.1	Isolation Test Results.....	9-31
9.3.4	Post-Qualification Tests.....	9-32
9.3.4.1	Setup and Check-Out Test Results	9-32
9.3.4.1.1	Operability Test Results.....	9-33
9.3.4.1.2	Prudency Test Results.....	9-33
9.4	Conclusion	9-33
10	Software Qualification	10-1
10.1	The Dedication of Pre-Developed Software (PDS).....	10-2
10.1.1	Software Commercial Grade Dedication Overview	10-2
10.1.1.1	Verification of Software Documentation.....	10-3
10.1.1.2	Documentation Evaluation.....	10-4
10.1.1.3	Software and Validation Testing Program.....	10-4

10.1.1.4	Operating History Evaluation	10-4
10.1.2	Verification of Software and Documentation	10-5
10.1.2.1	Software Requirements	10-5
10.1.2.2	Software Design Specification.....	10-5
10.1.2.3	Software Dedication Process	10-6
10.1.2.4	Source Code Inspection	10-7
10.1.3	Software Validation and Testing Program.....	10-7
10.1.3.1	Application Software Object Tests	10-8
10.1.3.2	Software Component Tests	10-9
10.1.3.3	Functional Tests	10-10
10.1.4	HFC-6000 Operating History	10-10
10.1.4.1	Operating History Background and Evaluation Approach	10-10
10.1.4.2	HFC Product Lines	10-11
10.1.4.3	Product line History	10-11
10.1.4.3.1	AFS-1000 Product line History	10-11
10.1.4.3.2	ECS-1200 Product line History	10-13
10.1.4.4	Relationship of HFC-6000 product line to the AFS-1000 product line.....	10-13
10.1.4.5	Relationship of HFC-6000 product line to the ECS-1200 product line.....	10-14
10.1.4.6	ECS-1200 Operating History	10-14
10.1.4.7	Module Operating Years (TMOY) calculation.....	10-17
10.1.4.7.1	Assumptions for TMOY Calculation.....	10-17
10.1.4.8	Determination on Critical/Non-critical Software Defects	10-19
10.1.4.9	Conclusions of defect analysis.....	10-20
10.1.4.10	Summary of Operating History.....	10-21
10.1.5	Software Operation and Maintenance.....	10-21
10.1.5.1	Error Detection.....	10-22
10.1.5.2	Error Correction Change Control.....	10-23
10.1.5.2.1	Change Management Levels of Authority.....	10-23
10.1.5.2.2	Software Change Request (SCR).....	10-23
10.1.5.2.3	Audits and Reviews	10-24
10.1.5.3	Training.....	10-24
10.1.5.4	Customer Reporting.....	10-24
10.1.5.5	QA & CR Process	10-24
10.2	Safety Related Software Development	10-25
10.2.1	Software Development Life Cycle.....	10-25
10.2.2	Life-Cycle Verification and Validation	10-28
10.2.2.1	Project Planning Phase.....	10-28
10.2.2.2	Requirement Phase.....	10-29
10.2.2.3	Design Phase.....	10-30
10.2.2.3.1	Product Development Project	10-30
10.2.2.3.2	Application Development Project.....	10-31
10.2.2.4	Implementation Phase.....	10-32
10.2.2.4.1	Product Development Project	10-32
10.2.2.4.2	Application Project	10-32
10.2.2.5	Integration and Testing Phase.....	10-33

10.2.2.6	Deployment.....	10-34
10.2.2.7	Operation and Maintenance	10-34
10.2.3	V&V REPORTING	10-34
10.2.3.1	V&V Task Report.....	10-35
10.2.3.2	V&V Analysis Report.....	10-35
10.2.3.3	Software V&V Report	10-35
10.2.3.4	Condition Reports	10-35
10.2.3.5	Final V&V Report.....	10-36

INDEX OF FIGURES

Figure 5-1 - HFC-6000 System Arrangement Diagram	5-1
Figure 6-1 - HFC-SBC06 controller I/O interface	Error! Bookmark not defined.
Figure 6-2 - Public Memory Data Stored	6-3
Figure 6-3 - HFC I/O Module Architecture	6-5
Figure 6-4 - ICL Communication Architecture	6-6
Figure 6-5 - C-Link and ICL Communication Networks	6-9
Figure 7-1 - The execution of software tasks on the system processor	7-5
Figure 7-2 - Communication Paths of HFC-6000 controller	7-5
Figure 7-3 - Secondary Loop Back Test	7-10
Figure 8-1 - Configuration for Critical Analog Signals	8-34
Figure 8-2 - Public Memory shared between C-Link and SYS processors	8-39
Figure 9-1 - Test Data Flow Chart	9-5
Figure 9-2 - Overall Test Sequence	9-6
Figure 9-3 - Environmental Stress Temperature Profile	9-18
Figure 9-4 - Test Spectrum	9-27
Figure 10-1 - Software Commercial Grade Dedication	10-3
Figure 10-2 - Software Operation and Maintenance	10-22

INDEX OF TABLES

Table 1-1 - The Base HFC-6000 System	1-2
Table 6-1 - List of HFC-6000 I/O Modules	6-6
Table 7-1 - HFC-6000 Safety software development and maintenance tools	7-13
Table 8-1 - Software Layers of C-Link processor	8-41
Table 10-1 - AFS-1000 Product line history	10-12
Table 10-2 - ECS-1200 Product line history	10-13
Table 10-3 - Key ECS-1200 Installations	10-14
Table 10-4 - TMOY Calculation	10-18
Table 10-5 - Operating history and defect hours	10-19

1 Introduction

1.1 Introduction to HFC

HF Controls (HFC), located in Carrollton, Texas, was established in 1961 as Forney Engineering Company and commissioned by Foster Wheeler to develop fossil plant control systems. In 1979 HFC entered the nuclear plant safety systems supply industry with the award of contracts for the Duke Power Cherokee 1&2 and Perkins 1&2 nuclear power plants. These contracts included the safety related control systems. The Duke Power control systems were 90% complete prior to cancellation of plant construction. Subsequently HFC was contracted by KEPCO in Korea to provide both safety related and non-safety digital control systems for the Yongwang 3 & 4 plants. These control systems, delivered in 1994, have experienced very reliable plant operation. In the years following Yongwang, HFC was contracted by KEPCO to supply the Ulchin 5 & 6 non-safety and safety related control systems. These systems were delivered in 2002 and 2003, and have also experienced very reliable plant operation. Although it was never constructed, KEPCO selected HFC to provide the KEDO plant safety related control systems. In addition to supplying a number of upgrades to nuclear and fossil operating plants in Korea, HFC provides I&C equipment support to over 450 power and industrial plants throughout the world.

HF Controls currently specializes in the design and construction of high reliability control systems for a variety of industrial, fossil power and nuclear power applications. Based on field-proven technology, HFC supplies its customers with a broad array of advanced control hardware that offer distributed intelligence and information management. HFC provides process control systems, technology, engineering, project management, and services.

The HFC control systems provided for the Yongwang 3 & 4 and the Ulchin 5 & 6 nuclear plants in Korea include non-safety and safety controls, I/O modules, data communication modules, power supplies, and control room HMI devices for the NSSS and BOP field components. To date HFC has provided the Korean nuclear power generation industry with over 4,000 individual controllers, with between 10,000 and 17,000 I/O points per plant in a highly functionally segregated and partitioned design. All systems were delivered on schedule, subsequently boasting exceptionally high reliability.

1.2 Introduction to HFC-6000

HFC currently supports two predecessor product lines: the AFS-1000 (Boiler Safety and Nuclear Safety I&C Systems) and the ECS-1200 (Plant Control System) on which the HFC-6000 (Nuclear Safety I&C System) design is based. HFC is requesting the NRC's review of the HFC-6000 product line for suitability in domestic safety related nuclear applications. The earlier ECS-1200 and AFS-1000 product lines have extensive fossil and nuclear power plant operating bases. Both HFC-6000 and ECS-1200 systems use basically identical software. The changes to develop the HFC-6000 hardware from the ECS-1200 hardware are associated with changes to the ECS-1200 form factor.

It is HFC's intent to employ this report as the vehicle by which HFC will receive the NRC's positive review of its control technologies which will enable domestic nuclear power plant licensees to reference the use of basic (i.e., as defined here) HFC-6000 hardware, software operating system, communication software, and I/O software in license applications for their safety system installation upgrades and future new nuclear plants. Review and approvals for specific plant applications will be addressed in plant-by-plant license applications.

In summary the base system described herein includes the redundant HFC-SBC06 controller and a specific set of HFC-6000 series input and output (I/O) modules. The HFC-SBC06 controller provides the process execution from the pre-defined control programs and updates the input and output signals respectively. The multiple channel I/O modules handle both digital and analog signals based upon the types of I/O devices. The HFC-6000 controller and associated I/O modules are microprocessor based printed circuit boards loaded with firmware. The communication between controller and I/O modules is via RS485 I/O communication Link (ICL). The connection medium can be either Fiber Optic media or twisted pair metal wires. The field proven HFC-6000 control software and I/O firmware referenced here is a qualified subset of the of Pre-Developed Software (PDS) software and firmware library that has been previously implemented on numerous nuclear safety applications. The C-Link communication provides a means for a controller to broadcast and receive information with other controllers in the same division and also to broadcast, but not receive, information with non-safety related equipment.

Table 1-1 provides a comprehensive list and description of the HFC-6000 base system.

Table 1-1 - The Base HFC-6000 System

Category	Module Type	Description	Processor
Hardware		HFC-6000 Controller Rack	N/A
Hardware	HFC-BPC19	HFC-6000 Controller Backplane	N/A
Hardware	HFC-BPE19	HFC-6000 Expander Backplane	N/A
Hardware and Software	HFC-SBC06	Redundant Controller Card Set	Control Input/Output Communication
Hardware	HFC-DPM06	Dual-Ported Memory for Redundant Controller	N/A
Hardware and Firmware	HFC-DI16I	16-Channel (Port) Digital Input Card	Input Processor
Hardware and Firmware	HFC-DO8J	8-Channel (Port) High Current Relay Output Card	Output Processor
Hardware and Firmware	HFC-DC33	Nuclear Power Plant Special Function Card with 2 channel 120-vac digital output and 12 channel digital input	Input/Output Processor
Hardware and Firmware	HFC-DC34	Nuclear Power Plant Special Function Card with 2 channel 125-vdc digital output and 12 channel digital input	Input/Output Processor

Hardware and Firmware	HFC-AI4K	4-Channel (Port) Pulse Input Card, High Resolution	Input Processor
Hardware and Firmware	HFC-AI16F	16-Channel (Port) Analog Input Card,	Input Processor
Hardware and Firmware	HFC-AO8F	8-Channel (Port) Analog Output Card	Output Processor
Hardware and Firmware	HFC-AI8M	8-Channel (Port) 100 Ohm RTD Input Card	Input Processor
Hardware	HFC-ILR06	I/O Link Fiber Optics Repeater/Terminator	N/A
Hardware	ECS-B232	Fiber Optic Transmitter	N/A

2 Documents and Definitions

The document structure used in the development and qualification of the HFC-6000 safety system include the following categories of interest:

- Topical Report and Related Documents submitted to the NRC
- HFC-6000 Qualification Project Documents
- QA Procedures and Related Documents
- HFC-6000 Product Line Documents

This structure constitutes a hierarchical document mapping system to guide the report's reviewers seeking data referenced throughout this report.

2.1 Definitions

Abnormal Conditions and Events (ACE). Postulated internal or external abnormalities that may affect performance of a system.

Acceptance Testing. Formal testing conducted to determine if a system satisfies its acceptance criteria and to enable a customer to assess the acceptability of the system.

Application Software. (1) Software designed to fulfill the specific needs of a user. (2) Software that performs a task related to the process being controlled rather than to an internal operation of the component itself.

Component Testing. Testing of hardware or software components or groups of related components conducted to verify the implementation of the design.

Computer. A programmable functional unit that consists of one or more associated processing units and peripheral equipment, that is controlled by internally stored programs, and that can perform substantial computation without human intervention during its processing sequence.

Computer Program. A combination of computer instructions and data definitions that enable computer hardware to perform computational or control functions.

Critical Component. Hardware or software integrated into control systems and instrumentation for a safety system. In this document, a *critical component* is synonymous with a *safety-related component*.

Design Basis Event. Postulated events used in the design to establish the acceptable performance required for structures, systems, and components.

Design Phase. The period in a project life cycle during which the designs for architecture, hardware or software components, interfaces, and data are created, documented, and verified to satisfy project requirements.

Design Inputs. The specific combination of functional and performance characteristics that a new design is required to fulfill. Design Inputs are also called Design Requirements.

Failure Modes and Affects Analysis (FMEA). A systematic evaluation of component responses to a postulated failure condition.

Form Factor. The hardware platform and backplane design for a computer system.

Implementation Phase. The period of a project life cycle during which hardware and software components are created from design documentation.

Integration Phase. The period of a project life cycle during which hardware and software components are progressively combined into their operating environment and tested in this environment to verify functional performance.

Life-Cycle Phase. Any period during a project that may be characterized by a primary type of activity being conducted. Different phases may overlap; for V&V purposes, no phase is complete until its development products are verified fully.

Regression Test. Selective retesting of a component following modification to correct an error or design problem. The purpose of such testing is to verify that the modification resolved the problem that had been identified without introducing any new problems.

Requirements Phase. The period of a project life cycle during which functional and nonfunctional requirements (design inputs) are defined and documented.

Software. Programs, procedures, rules, data, and any associated documentation pertaining to the operation of a computer system.

System Software. A computer program that performs tasks related to internal operation of the computer itself.

Traceability Analysis. A systematic method for tracing each requirement for a project to its final implementation in a project. The scope of such an evaluation may be restricted to a single life time phase, or it may encompass an entire project.

Validation. The process of evaluating an integrated computer system (hardware and software) or individual component during or at the end of its development process to determine if it satisfies specified requirements.

Verification. The process of evaluating a system or component to determine whether or not the products of a given development phase satisfies the conditions imposed at the start of that phase.

3 Acronyms

A	Ampere
AC	Alternating Current
ACE	Abnormal Conditions and Effects
ACK	Acknowledge
ADC	Analog/Digital Converter
AI	Analog Input
AMSAC	ATWS Mitigation System Actuation Circuitry
AO	Analog Output
AOT	Application Object Test
ASO	Application Software Objects
ATWS	Anticipated Transient Without Scram
BLRQ	Block Request
BOE	Burst of Events
BOP	Balance of Plant
C	Celsius; also Centigrade
CD	Compact Disk
CFR	Code of Federal Regulations
C-Link	Communication Link
CMS	Code Management System
CO	Category Owner
COMM	Communication Module
CPU	Central Processing Unit
CPUM	CPU Module
CQ4	HFC Analog Algorithm
CR	Condition Report
CRC	Cyclic Redundancy Check
CRG	Condition Review Group
CRT	Cathode Ray Tube
DAC	Digital/Analog Converter
dB	Decibel
dc	Direct Current
PCS	Plant Control System
PLC	Programmable Logic Controller
DDB	Dynamic Data Base
DF	Digital Flags
DI	Digital Inputs
DO	Digital Outputs
DPM	Dual Ported Memory
EMI/RFI	Electro-Magnetic Interference/Radio Frequency Interference
EOB	Electrically Operated Breaker
EPROM	Erasable Programmable Read Only Memory

ESD	Electrostatic Discharge
ESFAS	Engineered Safety Features Actuation System
EWS	Engineering Workstation
F	Fahrenheit
FL	Flags
FMEA	Failure Modes and Effects Analysis
FO	Fiber Optic
FOT	Fiber Optic Transmitter
GDC	General Design Criteria
H	Hertz
HAS	Historical Archiving System
HFC	HF Controls
HMI	Human Machine Interface
HPAT	HFC Plant Automated Tester
H/W	Hardware
Hz	Hertz
I&C	Instrumentation and Control
ICL	Intercommunication Link
ID	Identification
IEEE	Institute of Electrical and Electronics Engineers
I/O	Input/Output
IOM	Input/Output Module
ISG	Interim Staff Guidance
KEDO	Korean Peninsula Energy Development Organization
KEPCO	Korean Electric Power Company
KHz	Kilo Hertz
LED	Light Emitting Diode
LLC	Link Logic Control
mA	milli Ampere
MAC	Medium Access Control
MCL	Master Configuration List
MFM	Master for a Moment
MHz	Mega Hertz
μ	Micron
μ V	Micro Volt
MMI	Man Machine Interface
MMS	Module Management System
MS	Microsoft
MSS	Maintenance Subsystem
MTBF	Mean Time Between Failures
MUX	Multiplex
NACK	Negative Acknowledge
NIC	Network Interface Chip
NRC	Nuclear Regulatory Commission
NSSS	Nuclear Steam System Supplier

OBE	Operating Basis Earthquake
OEM	Original Equipment Manufacturer
OIS	Operator Interface System
OS	Operating System
PC	Personal Computer
PCB	Printed Circuit Board
PCS	Plant Control System
PDS	Previously Developed Software
PLC	Programmable Logic Controller
PMS	Plant Monitoring System
PO	Purchase Order
PROM	Programmable Read-Only Memory
PSM	Power Supply Module
QA	Quality Assurance
QAPM	Quality Assurance Program Manual
QC	Quality Control
RAD	Unit of Radiation
RAM	Random Access Memory
RELEX	Reliability Program
RF	Radio Frequency
RG	Regulatory Guide
RH	Relative Humidity
RMS	Root Mean Square
ROM	Read-Only Memory
RPS	Reactor Protection System
RRS	Required Response Spectrum
RTD	Resistance Thermal Detector
RTS	Reactor Trip System
SAR	Safety Analysis Report
SBC	Single Board Computer
SC	System Controller
SCM	Software Configuration Management
SCR	Software Change Request
SDD	System Design Description
SDP	Software Development Plan
SLC	Single Loop Controller
SMT	Software Management Team
SIP	System Integration Plan
SOE	Sequence of Events
SQAP	System Quality Assurance Plan
SQL	Microsoft Server Utility
SRS	System Requirements Specification
SSE	Safe Shutdown Earthquake
SSP	System Safety Plan
Std	Standard

STP	System Test Plan
SVVP	System Verification and Validation Plan
SVVR	System Verification and Validation Report
S/W	Software
SYS	System CPU
TCB	Task Control Block
TRS	Test Response Spectrum
TSAP	Test System Application Program
TCP/IP	Transmission Control Protocol/Internet Protocol
UCN	Ulchin Nuclear Power Plant
UCP	Universal Communication Packet
UDP	Universal Data Packet
UFSAR	Updated Final Safety Analysis Report
UPS	Uninterruptable Power Source
v	Volts
vac	Volts Alternating Current
VAX	Digital Computer
vdc	Volts Direct Current
YGN	Yongwang

4 Overview of HFC-6000 Qualification Project

The HFC-6000 system design requirements were established using the earlier AFS and ECS product lines design requirements with minor modifications where needed. Functional, environmental, module interface and performance requirements were established for the HFC-6000 system to be compatible with the USA nuclear installations and the associated plant digital control systems upgrade requirements. These requirements form the bases for the design of the system and with their specification defines the key areas for design reviews including audits and verification and validation processes. The Qualification Project was performed using the regulations, codes, standards and, guidance as discussed in Section 8.5 that are applicable to the design and qualification of digital safety systems and the scope of this Topical Report.

The technical scope and content of EPRI TR-107330 are focused on defining a series of steps needed to complete a generic qualification program. Accomplishing the qualification requires creation of a synthetic application, so the steps are similar to those in qualifying a device for safety-related service. For the HFC-6000, these steps and associated HFC qualification tasks were performed as defined in this document. The specific steps included;

- A. Define an architecture overview of the HFC-6000 system and evaluate the suitability for the intended application, Input/Output modules, communication, and controller modules were defined so as to encompass a broad range of nuclear applications. This review also included the performance of a single failure analysis considering redundancy that would be incorporated in the plant design. Using this architecture, a Failure Modes and Effects Analysis (FMEA) for the HFC-6000 system was performed. This is to be used in the future as an input to the more detailed plant specific application and overall FEMA. This overview included an analysis of the deterministic features of the system.
- B. Evaluate the HFC-6000 system's hardware and software QA programs that are applied to determine if they are adequate to support nuclear safety-related applications with a reasonable set of supplementary activities. The evaluation includes factors relating both to generic qualification and future potential applications of the qualified products.
- C. Select a set of modules, supporting devices and software from the HFC-6000 system to be used as the qualification test specimen and included in qualification project.
- D. Define and produce a Test System Application Program (TSAP). The TSAP serves as a synthetic application that is designed to aid in the qualification tests and demonstrate the acceptability of the system being qualified.
- E. Combine modules of the Test Specimen and the TSAP into a suitable test configuration and perform a set of acceptance tests. This activity constitutes the system integration testing for the Test Specimen.

- F. Specify the set of hardware qualification tests to be performed on the Test Specimen, including a defined set of tests to be conducted at suitable times in the qualification process.
- G. Perform the hardware qualification tests, perform the data analyses, and document the results. Results documentation includes definition of the qualification envelope, identification of the specific products that were qualified, and guidance for using the qualified system in a specific application.
- H. Perform a suitability analysis for HFC-6000 requirements including such features as accuracy, response times and physical characteristics. Identify all I/O points, scan rates and software features.
- I. [
- J.
- K.]
- K. Develop the test application software using the HFC quality standards. The HFC development process is mature and stable and provides safety related application software that meets all guidelines and regulations applicable to the scope of this report.
- L. Ensure that the configuration identification and management program for the HFC-6000 hardware and software is maintained using the guidelines contained in the applicable standards and regulations.
- M. Ensure that all specifications of the HFC-6000 system are consistent with the requirements of 10 CFR 50 Appendix B, IEEE Std 603-1991 and the applicable GDCs. Ensure that all applicable RGs and industry standards have been followed or adequate justification provided.

]

HFC requests that the NRC review the HFC -6000 platform as described in this Topical Report. This includes the hardware and software defined in this report. The following sections of this report will provide both design and qualification details that will demonstrate compliance with all applicable regulations for a programmable safety related instrumentation and control system.

5 HFC-6000 System Overview

HF Controls provides a programmable logic controller to support nuclear power plant safety, control, and information functions. The HFC-6000 digital safety system was designed to meet regulatory requirements for safety system applications. These include component quality, hardware and software qualification, redundancy, fault tolerance, deterministic performance, isolation and independence. The overall architecture of HFC-6000 control and information systems form the bases to meet the requirements for nuclear power plant applications.

The primary CPU Module (CPUM) in a HFC-6000 controller unit is the system controller (HFC-SBC06), which supports the execution of control logic programs, and I/Os scan and C-Link communication. [

]

The Power Supply Module (PSM) represents the redundant rack mounted power supply set. This hot swappable redundant power supply provides 24 vdc for both controller and I/O modules. [

] Figure 5-1 - HFC-6000 System Arrangement Diagram

6 HFC Safety I&C Platform Hardware Description

This section provides an overview of the hardware components that make up the HFC-6000 nuclear safety I&C platform. They include various I/O, communication, power supply and controller modules and chassis. The software for the various modules is discussed in Section 7. This product line has been developed as a generic I&C application having a medium density I/O (up to 1000 points per controller). The scope of potential applications includes safety-related control functions for nuclear power plants.

6.1 System Controller Module

The HFC-6000 safety system provides plant monitoring and control functions, with monitoring and control capabilities. The HFC-SBC06 System Controller is the primary module used for implementing plant safety functions. The HFC-SBC06 System Controller module is positioned in the HFC-6000 safety system between the human machine interfaces through the I/O modules, which provide the signal-level interface to the equipment and devices under monitoring or control. Figure 6-1 shows the interface function for a single safety division of the HFC-SBC06 controller between its onboard system processor and its communications processors.]

]

Descriptions of the functional requirements of the HFC-SBC06 System Controller module and HFC-DPM06 Dual Ported Memory module, from an external perspective, are provided in the HFC-6000 Product Line Requirements Specification, RS901-000-01. Detail level descriptions of the HFC-SBC06 and HFC-DPM06 are contained in the HFC-SBC06-DPM06 System Controller Module Detailed Design Specification, DS901-000-01. Additional C-Link design discussions are in Sections 6 and the compliance with interim staff guidance on communication issues is contained in Section 8.

[

]

6.2 Input /Output Modules

The HFC-6000 I/O modules provide signal-level interface to the equipment and devices which are being monitored or controlled. The major functions performed by the HFC-6000 I/O modules are:

- Measuring input signals or setting output signals
- Communication with HFC-SBC06 system controller through the ICL
- Self-diagnostic functions

[

] Table 6-1 provides a list of the current HFC-6000 I/O module types and a description of the I/O channels for each module type. Some module types have a combination of input and output points.

Table 6-1 - List of HFC-6000 I/O Modules

Name	I/O Channels (Ports)
DO8J	8 channel digital relay output
DI16I	16 channel digital input
DC33	2 channel 120-vac digital output and 12 channel digital input
DC34	2 channel 125-vdc digital output and 12 channel digital input
AI16F	16 channel analog input
AO8F	8 channel analog output
AI8M	8 channel 100 Ω RTD input
AI4K	4 channel pulse input

The overall architectural design of standard HFC-6000 I/O modules and its standard functions are provided by document MS901-000-02, "HFC-6000 I/O Module Design Specification." The design descriptions of the common software modules of I/O modules are described in document DS901-000-02, "HFC-6000 I/O Module Detailed Design Specification."

6.2.1 Relay Output Module

The HFC-DO8J assembly is an eight-channel relay digital output module. [

]

6.2.2 Digital Input Module

The HFC-DI16I assembly is a 16-channel digital input module. [

]

6.2.3 Digital Controller Module

The HFC-DC33 is a special purpose, multi-channel I/O buffer module designed for nuclear power plant applications. It is used by the HFC-6000 for control, interrogation, and monitoring of field devices. This buffer is specifically designed to meet the unique control requirements of a dual-coil Motor Operated Valve (MOV) starter. Typical applications include controlling dual coil motor starters while monitoring coil continuity, overloads and valve position.

[

]

6.2.4 Digital Control of Breakers Module

The HFC-DC34 is a multi-channel Input/Output (I/O) buffer printed circuit module (PCB). It is used for control, interrogation, and monitoring of field devices in a HFC-6000 control system. 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.

[

]

6.2.5 Analog Input Module

The HFC-AI16F module operates as a standard AI module in a HFC-6000 control system. [

]

6.2.6 Analog Output Module

The HFC-AO8F module operates as the standard AO module in a HFC-6000 control system [

]

6.2.7 RTD Input Module

The HFC-AI8M Resistance Temperature Detector (RTD) printed circuit module (PCB) is an input-conditioning device for a HFC-6000 control system.[

]

6.2.8 Pulse Input Module

The HFC-AI4K module provides four input channels for processing pulse signals from field equipment.[

]

6.3 *Communication Modules*

In an HFC-6000 System, C-Link communication and ICL communication support are integrated in the system controller modules and I/O modules. Figure 6-5 depicts the configuration.]

] The purpose of the C-link is to provide operational information/data from a controller in a division to other controllers in the same division on the C-Link and to also provide operational information/data to non-safety related equipment through one-way communication devices attached to the C-link.

The ICL links handle communication between the HFC-SBC06 system controller module and its I/O modules.

[

]

6.4 Power Supplies and Chassis

The HFC-6000 product line provides a rack-mounted power supply module with slots for separate power supplies. The rack-mounted power supply module can accommodate up to eight separate (four redundant) power supply assemblies, and each set of power supplies can be connected to a different power source. The power capacity of this arrangement is adequate to supply operating power for eight, or more, fully loaded HFC-6000 controller chassis.

Each HFC-6000 cabinet includes power supply modules in a separate power rack that provides redundant 24-vdc and 48-vdc power via separate backplane traces. Since the power supply modules are redundant, the loss of one module will not degrade functional operation of the I&C system as a whole.

There are two types of backplanes in the HFC-6000 product line: the HFC-BPC01-19 and the HFC-BPE01-19.

HFC-BPC01-19 is a controller chassis backplane for a 19-inch equipment cabinet. It offers two slots for HFC-SBC06 system controllers, one slot for an HFC-DPM06, and capacity for a maximum of 11 HFC-6000 I/O modules. The backplane can receive operating power from redundant power cables that attach to a connector on the back of the chassis. The system controller(s) plugged into this backplane communicates with I/O modules via redundant serial Intercommunication Link (ICL) traces on the backplane. Redundant ICL connectors on the rear of the backplane card enable connection of the ICL with an expansion card chassis.

HFC-BPE01-19 is an I/O expansion chassis backplane for a standard 19-inch equipment cabinet assembly. It provides slots for a maximum of 14 HFC-6000 I/O modules. The backplane can receive operating power from redundant power cables that attach to a connector on the back of the chassis. The ICL cables from a controller chassis mate with connectors on the back of the card, and ICL traces are routed to the connector for each card slot.

The structures of all HFC-6000 card chassis are designed to meet category 1 seismic requirements.

7 HFC Safety Platform Software Description

The software that will be utilized for safety related applications of the HFC-6000 is broken down into the following categories:

- Operating Software
- Application Software (Plant Specific)

Operating software consists of firmware programs that provide the generic operating capability of the HFC-6000 product line. This generic firmware is written in Assembly language stored in non-volatile memory and is not alterable by the end user. The Operating Software has been in use for a number of years and is commercially dedicated as discussed in Chapter 10 of this report. The operating software for the HFC-6000 is discussed in detail below.

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 and cannot be altered while the controller is operating in the on-line mode. The Applications software is written in accordance with BTP 7-14 and this process is discussed in Chapter 10 of this report.

Application software is created or modified with the use of an off-line Engineering Workstation (EWS) in accordance with a pre-established software development processes. The new or modified software can only be installed in one controller of a redundant set at one time. This new or modified Application software meets the guidance provided in BTP 7-14. The controller has to be in the off-line mode for installation.

This section consists of the following platform Operating Software topics:

- Controller Software
- Inter-Communication (ICL) Software
- The Development and Maintenance tools
- Communication Link (C-Link) Software

7.1 Controller Software

7.1.1 HFC-SBC06 Controller

The HFC-SBC06 controller module has a Pentium system (SYS) processor and two 32-bit subordinate microprocessors, each of which has a separate independent firmware programs installed in its private memory array. [

]

7.1.1.1 The System (SYS) Processor

The SYS processor has access to the flash memory that consists of installed application programs. The application program consists of a sequential set of instructions that are executed by the Equation Interpreter software task. [

]

7.1.1.2 SYS Processor Software Architecture

The SYS Processor software design is composed of a generic real-time Operating System (OS) and a set of configurable tasks that will be run by that operating system. The OS is mainly a deterministic task scheduler; that executes the configured tasks one after another according to a task control block (TCB) list. [

]

7.2 *Communication Software*

[

]

7.2.1 Communication Link (C-Link) Software

The C-Link processor of the controller is responsible for regulating messages sent over the C-Link.[

]

7.2.1.1 Message Types

[

]

7.2.1.2 Token Passing Scheme

[

]

7.2.1.3 Synchronization on Dual-Channels

[

]

7.2.1.4 Deterministic Nature of the C-Link

[

1

7.2.2 ICL Communication Software

The ICL protocol is an HFC proprietary design used for general communications between a controller module and its configured I/O modules.

7.2.2.1 I/O module communication

[

]

7.2.2.1.1 Redundant Serial Link

Each HFC-6000 controller includes a hardware interface for one or more ICL channels to provide the hardware link with configured I/O modules. All I/O modules include a redundant ICL interface to permit communication with the redundant controllers. During initialization, one controller becomes Primary, and the other becomes Secondary.]

]

7.2.2.1.2 Polling Operation

The ICL employs a poll-response communication protocol to control message exchanges between the controller and its configured I/O modules.]

]

7.2.2.1.3 Secondary Loopback Test

The ICL protocol supports secondary loopback tests for HFC-6000 controllers operating in a redundant configuration. The purpose of these tests is to verify the functional operation of the secondary link with each station. [

] Figure 7-1 - Secondary Loop Back Test

7.2.2.1.4 Secondary Polling Function

If an I/O module does not respond to a regular poll message, the Primary controller will request the Secondary controller to poll the same I/O module.[

]

7.2.2.1.5 ICL Software Architecture

The ICL Processor software is designed based on the operating system component common to the SYS processor on the HFC-SBC06 module and a set of configurable tasks that will be run by the operating system.

[

]

7.2.3 Input/Output Module Firmware

[

] The firmware code controls initialization, diagnostics, ICL communication, I/O scan, and data processing functions. The initialization, diagnostics and ICL communication functions are identical for all I/O module types. The characteristics of the I/O scan and data processing functions are uniquely configured for each module type, and the hardware initialization code is designed to operate with the specific hardware components that make up that module.

The program algorithm for each I/O module automatically accesses the initialization routine immediately following power-up. This routine performs hardware and firmware validation checks and then transfers control to the initialization routine. [

] Between successive I/O scan cycles, the main program runs diagnostic checks as a background operation.

All I/O modules are configured as slave stations on the ICL.[

] If the data is valid, the routine returns the message in the current response buffer, transfers any message data received from the controller to memory, and then returns control to the main program.

[

] Hardware timer is used to control I/O scan intervals, communication response time out, etc. When a timer interrupt occurs, the configured Timer Interrupt Service Routine handles the interrupt.

7.3 The Development and Maintenance Tools

The firmware for the controllers and I/Os of HFC-6000 safety platform software is written in Intel Assembly language. It was developed under Intel x86 Cross Assembler, Linker and Locator on a Digital VAX computer. [

]

Table 7-1 illustrates the HFC-6000 software development and maintenance tools. The code management was implemented through Digital Code Management System (CMS) for original source codes and Microsoft SourceSafe and utility software is the current configuration management tool. All listed development tools from Intel x86 Assembler, Linker and Locator are Intel products and used by HFC over the past twenty plus years. [

]

Table 7-1 - HFC-6000 Safety software development and maintenance tools [

The "Generation" and "Class" are CMS and MMS library utilities to manage the version and change process of software files and configuration. HFC uses "Class" to define the product line or project and uses "Generation" to dedicate a version of software files for a particular "Class".

The detail description on Software Operation and Maintenance is specified in the Section 10.1.5.

These software development and maintenance tools are managed under the HFC Configuration Management Procedure, and any error produced would be discovered under the HFC Software V & V program. Furthermore, the accuracy of these tools is validated through the historical use by HFC and other industries and also by the HFC tool validation program.

8 Safety System Design Topics

8.1 Deterministic and Time Response

A nuclear power plant safety system that utilizes the HFC-6000 product line must provide deterministic performance with predictable operation and defined maximum response time characteristics. This means that the calculated cycle time will be repeatable each and every cycle. This section will address the internal operation of a single channel or division, and will describe aspects of deterministic performance as it relates to the external interfaces with other redundant elements. Each independent channel and division of an HFC safety system will include an independent external hardware watchdog timer to monitor the deterministic performance and initiate the appropriate fail-safe action if it is not reset within a predetermined interval.

This description will define all aspects of deterministic performance including:

- System Controller
- System Processor Characteristics
- ICL Processor Characteristics
- I/O Module Characteristics
- C-Link Processor

8.1.1 System Controller

An HFC safety system is configured with redundant System Controllers. With a redundant System Controller configuration, a second System Controller and a Dual Ported Memory Board are required. One controller is in the primary control mode and the other is in the secondary mode. The secondary mode controller monitors the primary System Controller and updates its database through the DPM. If the primary controller fails, the secondary controller takes over the operation.

[

8.1.2 SYS Processor Characteristics

The real-time operation of the SYS processor is controlled by a task scheduler.]

]

8.1.2.1 Applications Tasks

The SYS processor performs the safety-related applications processing as scheduled by the real time tasks.[

]

8.1.2.2 Supervisory Tasks

The SYS processor performs self-diagnostics as a lower priority task than the safety-related applications. Error conditions are logged for system status determination. [

]

8.1.3 ICL Processor Characteristics

The ICL processor operation differs depending on whether it is operating in the primary controller mode or in the secondary controller mode.

8.1.3.1 Operation in the Primary Controller

The ICL processor controls two serial interface channels for communication with I/O modules connected on the serial I/O link.[

] Similar to the SYS processor, the ICL processor performs periodic diagnostics and passes the diagnostic status to the SYS processor.

8.1.3.2 Operation in the Secondary Controller

In the standard redundant configuration, the ICL processor on the primary controller performs the periodic I/O polling. The ICL processor on the secondary controller only performs I/O operations at the request of the primary ICL processor. There are two operations that the ICL processor on the secondary controller is permitted to perform:

[

] This capability provides a level of fault tolerance to the I/O process, while maintaining deterministic performance of I/O operations.

8.1.4 I/O Module Characteristics

An I/O module is an independent card in the chassis. Each I/O module has a microprocessor. All I/O modules use a common protocol for communication with the ICL processor of the controller.

[

]

8.1.5 C-Link Processor Characteristics

The redundant C-Link communication design utilizes a token passing protocol for deterministic communication with other safety systems within its own division.

[

]

8.1.6 Deterministic Performance Conclusion

The HFC-6000 system is designed to have deterministic performance with a predetermined maximum response time to changing input signals and messages communicated locally and remotely. It is accomplished from the deterministic data scan scheme and fixed communication structure. The input signals are scanned by input modules in a fixed scan rate.]

]As noted above, the C-Link architecture is designed to be deterministic without handshaking or interrupts. The HFC-6000 communication scheme provides the deterministic characteristic to process the control signal from input device to output device.

8.2 Failure Mode Effects Analysis (FMEA)

The HFC-6000 System FMEA covers the existing system design for the HFC-6000 product line as described earlier in this report. The FMEA as presented in Tables A-1 through A-17 of the FMEA report, RR901-000-01-Rev C, was performed in accordance with EPRI TR-107330, Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants, Section 6.4.1, and the more detailed qualitative guidance in IEEE Std 352-1987, IEEE Guidance for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems. In general, the guidance and descriptions provided have been used in this analysis. These techniques included definition of system functional areas for the HFC-6000 operation, as listed in the FMEA Appendix. The postulated failure effect on each functional area was then analyzed, as summarized in Section 4.0 of the FMEA report.]

] A summary of the impact on system performance is presented in Section 4.2 of the FMEA report. The HFC FMEA evaluated the effects of failures within HFC-6000 system components and the ensuing effect on system safety functional performance. The existing HFC-6000 System design provides confidence that all failure conditions are detectable or that, for certain failures, the HFC6000 System redundant components permit continued operation of critical system functions in the presence of automatic switchover.

The FMEA analysis was performed on the HFC-6000 system components and configuration as proposed in the system hardware descriptions in this qualification report. This includes the controller, the I/O modules, the C-Link communication network and the ICL communication network. The analyzed configuration simulates a single channel of a typical nuclear system installation for a safety channel implementation.

The objective of the FMEA report is to document the methodology and results of the failure modes analysis for the HFC-6000 platform. Attachment A of FMEA provides tables showing the postulated failure mode, the possible causes, the symptomatic effects, method of detection, the effect of the failure on the system and the method of remediation.

[

] The HFC-6000 FMEA was used to identify postulated failure states for the HFC-6000 system. This analysis does not address failure modes associated with application of multiple PLC systems in redundant safety divisions. A typical plant design, since safety systems are always single-failure proof, provides for redundancy by implementing a three or four channels configuration. Although plant-specific mitigating design features are described for certain of the postulated failures, these features would have to be verified during a plant-specific application and its resulting FMEA.

[

]

The results of the FMEA should be applied to each plant-specific safety system design to disclose any potential hazard that will require additional mitigation for that application.

8.3 Reliability and Availability

A reliability and availability analysis was performed on the HFC-6000 product line for use in nuclear safety-related applications. For purposes of the analysis the Test Specimen configured for qualification testing was used. This configuration includes all the typical modules of the HFC-6000 control system.]

] The basic set of HFC-6000 I&C is composed of system controller modules, I/O modules, ICL link, C-Link and power supply modules. The system configuration required by Article 4.2.3.2, EPRI TR-107330 is used to perform the availability analysis.

Both EPRI TR-107330 and IEEE Std 352-1975 have been extensively used as guidelines in performing this reliability analysis. MIL-HDBK-217F was used for reliability prediction of individual parts that have been used to build HFC-6000 products. A software tool, RELEX software was used to perform the MIL-HDBK-217 Analysis on parts and assemblies of the HFC-6000 product line. RELEX software is one of the leading software tools for reliability and maintainability analysis. It provides software solutions for reliability predictions and MTBF calculations, which provide the basis for reliability evaluation and prediction.

[

] Mean Time to Repair has a strong influence on the availability that the equipment can achieve, but it is only partially under the control of the manufacturer. The best the manufacturer can do is to make the equipment easy to diagnose and repair. The owner has the responsibility to aggressively monitor the equipment for failure and expeditiously replace any part that fails. The owner also has the responsibility to maintain the system according to HFC's maintenance manual and replace modules according to the recommended replacement schedule.

Each system can have a different configuration and architecture. The reliability of the overall system is highly influenced by the choice of configuration and architecture design. From the system design side, there are two ways to improve availability of overall system: one is to select high reliability parts and products for the product line design, and the other is to utilize

redundancy in system design and configuration. Availability is improved significantly when redundancy is applied. HFC-6000 products provide redundancy support at different levels of the system. They can be used to build safety related control system with different configurations. The owner's decision on selecting the system configuration will decide the final availability of the overall system.

8.4 Quality Assurance Programs

The HFC Quality Program provides the administrative measures and procedures necessary to assure that all HFC hardware and software products as well as its support services meet or exceed all applicable guidance and regulatory guidelines. This Quality Program complies with

- ANSI/ASME NQA-1&1a-1994; "Quality Assurance Requirements for Nuclear Facilities"
- ANSI/ASME NQA-1a-1995 Addenda
- 10 CFR 50 Appendix B; "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants"
- ANSI/ISO/ASQ Q9001-2000, "Quality Management Systems - Requirements".

Software quality was verified per the guidance of ANS/IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations which incorporates guidance from ASME NQA-2a-1990 Part 2.7.

The HFC software quality assurance plans follow the guidance of IEEE Std 730-1984, "IEEE Standard for Software Quality Assurance Plans" and IEEE Std 983-1986, "IEEE Guide for Software Quality Assurance Planning".

Measures to assure the quality management of the software life-cycle were patterned after those described in HICB BTP-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems". HFC-6000 Verification and Validation efforts follow those described by IEEE Std 1012, "IEEE Standard for Software and Verification and Validation Plans".

Pre-Developed Software quality was verified using the commercial software guidance of IEEE Std 7-4.3.2, EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Equipment for Nuclear Safety Applications" and TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety Related Applications in Nuclear Power Plants."

The HFC QA program assures that the HFC-6000 design meets the requirements of

- Criterion 1, "Quality Standards and Records",
- Criterion 21 "Protection System Reliability and Testability" of Appendix A and
- Appendix B of 10 CFR 50.

Furthermore, IEEE Std 603, which requires that the quality of components be achieved through the specification of requirements known to promote high quality, was adopted as the basis from which HFC developed its requirements for design, inspection and testing. HFC has assumed the responsibility, as an Appendix B vendor, to comply with the regulations of 10 CFR 21. All applicable defects of HFC-6000 components are part of the HFC Part 21 notification process.

The HFC QA Program covers the design, implementation and commissioning of the HFC-6000 system. Requirements of this program apply to all activities (systematic and planned actions) affecting the quality of products and services provided and performed by HFC. The essential prerequisites for an effective quality assurance program were all incorporated into the QA program.]

]

To assure that the QA Program was being rigorously adhered to the Programs mandated; an independent verification effort to assess compliance with the QA Program and to provide on-going assessment of the adequacy of the measures was undertaken to ensure technical correctness of the QA processes.

The HFC Quality Assurance Manager has the responsibility for establishing the Quality Assurance Program and verifying that activities affecting the quality of deliverables are performed in accordance with this program. The performance of the group, that the manager represents, is assessed independent from the costs and schedule impacts of the group's mandated quality assurance measures. By reporting directly to the President of HFC, the Quality Assurance Manager is afforded sufficient authority and organizational freedom, to identify quality problems; to initiate, recommend, or provide solutions to quality problems; and to verify implementation of solutions to quality problems. Per the HFC QA Program, all employees share the same responsibility and authority as the QA Manager to identify quality problems; to initiate

and provide solutions to quality problems; to verify implementation; and to resolve deficiencies that affect quality.

As a minimum, formal management review of the quality system is performed annually to ensure its continuing appropriateness and effectiveness in satisfying HFC's business policies and objectives. Records of the management review meeting and associated completed action items are maintained in accordance with documented procedures.

HFC has established and maintains documented procedures to ensure that applicable regulations, codes, standards, and customer requirements are translated into design documents, procedures, and/or instructions. These documents include provisions to assure that appropriate quality standards are specified and included in design documents and that deviations from defined requirements are controlled.

As noted earlier, organizational and technical interfaces between different design group disciplines are defined by the Project Quality Plan. All design information communicated between the respective disciplines necessary to ensure satisfaction of these interface requirements is documented and regularly reviewed.

The design control program is established and implemented to assure that the activities associated with the design of systems, components, structures, and equipment and modifications thereto, are executed in a planned, controlled, and orderly manner. The program includes provisions to control design inputs, processes, outputs, changes, interfaces, records, and organizational interfaces. Major elements of this program include the following measures:

- Design input requirements, relating to the HFC products, are established, documented and their selection reviewed and approved for adequacy.
- Design outputs are documented and expressed in terms that can be verified against design input requirements and validated.
- Individuals or groups other than those that performed the original design review output documents.
- Independent design reviews occur at prescribed stages within the design process. Participants at each design review include, when necessary, representatives of all functions concerned with the design stage being reviewed.
- Records of design reviews are maintained.

Design verification includes design reviews, alternate calculations, qualification tests or a combination of methods executed in accordance with approved procedures. Design verifications are performed in accordance with approved procedures, performed prior to release for procurement, manufacturing, or to another organization for use to ensure that the design output meets the design input requirements. Independent design validations ensure that developed products conform to the specified requirements.

Design Analyses are performed in a planned, controlled and documented manner. They are sufficiently detailed as to purpose, method, assumptions, design input, references and units.

Methods such as computer programs and calculations are described and controlled. Qualification testing demonstrates adequacy of performance under conditions that simulate the most adverse design conditions.

Design changes are subject to design control measures identical to those applied to the original design. Design documents, including revisions, are reviewed, approved, released, distributed, and controlled in accordance with prescribed procedures and/or instructions. The HFC Software Configuration Management Program provides a method to track all past, current and future software configurations. This is discussed in more detail in HFC SCM documents.

8.5 Regulations, Codes, Standards and Guidance for Digital System Implementation

8.5.1 General

Listed below are those regulatory documents, codes, standards, and regulatory commitments that are applicable to the design, documentation, review, procurement, manufacture, installation, testing, operation, modification and maintenance of digital systems and their components and constituent parts for implementation in operating nuclear power plants.

8.5.2 Compliance with Nuclear Regulatory Commission (NRC) Documents

RG 1.22 1972 “Periodic Testing System Actuation Functions”

The HFC-6000 platform conforms to this Regulatory Guide (RG). Design principles have been employed that facilitate periodic testing of the HFC system to verify its ability to perform protective initiation functions. The HFC system allows complete testing of its actuated devices in accordance with the RG. This testing can be done with the plant at power or shutdown. An additional level of HFC-6000 testing is provided by diagnostic testing. A plant specific implementation will provide further details regarding periodic testing.

RG 1.29 “Seismic Design Classification”

The HFC-6000 system is qualified as a safety related system. As such, it is designated as a Seismic Category I system. The system is qualified by type testing to the required OBE and SSE levels. This is discussed in detail in the seismic qualification report (Section 9).

RG 1.47 1973 “Bypassed and Inoperable Status Indications for Nuclear Power Plant Systems”

Bypass and inoperable status information will be provided on a plant-specific basis.

RG 1.53 2003 “Application of the Single Failure Criterion to Nuclear Power Plant Systems”

Single failures of the HFC-6000 system have been evaluated in the earlier discussed FMEA summary. That assessment led to the conclusion that the system will meet the single failure criterion of IEEE-603 upon a plant specific implementation in a redundant safety system. Due to plant specific system redundancies, a plant specific implementation will provide the required information.

RG 1.62 1973 “Manual Initiation of Protective Actions”

All HFC-6000 actuation functions can be initiated manually. Provisions for this are maintained at the system level. However, provision for component level manual actuations will also be retained through past control system designs. The manual initiation path remains a relatively simple design. Details regarding manual initiation designs should be reviewed during the plant specific design reviews.

RG 1.75 2005 “Physical Independence of Electrical Systems”

The design of the HFC-6000 system conforms to this RG. The field-implementation of the HFC-6000 (e.g., the connecting wires, cables, switches and relays) will also conform to the physical, mechanical and electrical separation standards provided by the guide. A plant specific implementation will provide further details regarding physical independence.

RG 1.89 1984 “Qualification for Class 1E Equipment for Nuclear Power Plants”

The HFC-6000 system has been tested to verify its conformance with this RG, RG 1.209 and IEEE Std 323. The environmental qualification tests employed both type-testing and analysis which were followed per the provisions of EPRI TR-107330. This is described in more detail in Section 9 of this report.

RG 1.97 Rev 4 2006 “Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants”

The HFC-6000 controller and its I/O modules provide the flexibility and processing capability to accommodate a wide range of both analog and digital user instrumentation. The particular combination of instrumentation and controls that will be needed to detect and respond effectively to an accident condition will depend on the specific safety system being implemented. Consequently, this will be addressed on a project-by project basis.

RG 1.118 1995 “Periodic Testing of Electric Power and Protection Systems”

The HFC-6000 platform includes the following features built into the system hardware and software for direct verification of field equipment: [

Additional utilities for periodic testing of safety systems will be implemented as part of a specific application on a project-by-project basis. All such testing utilities will be designed in conformity with this RG, IEEE Std 338 and HICB-17 as discussed in the RG 1.22 discussion below.

RG 1.152 Rev 2 2006 “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants”

The HFC-6000 system design follows the guidance of this RG by meeting the applicable provisions of IEEE-ANS-Std 7-4.3.2. The software for the HFC-6000 is segregated into both pre-developed and new (application) software. For the new safety related software, HFC has implemented acceptable methods employed for designing, verifying, validating and implementing software to be used in safety related systems. The HFC software quality plan is consistent with this RG, the IEEE Std and ASME NQA-2a; this plan addresses all of the runtime resident computer software. The verification and validation processes are in accordance with applicable guidance. Those processes provide adequate confidence that the safety requirements and the requirements defined at each phase of the development process are implemented. The Pre-Developed Software is qualified based on the provisions of Section 5.3.2 and Appendix D of the IEEE Std. This qualification was also developed per the guidance of EPRI TR-106439 and TR-107330. Section 10 of this report provides detailed information on the qualification of the pre-developed software and the newly developed software.

RG 1.153 1996 “Criteria for Safety Systems”

This RG endorses IEEE Std 603-1991. It establishes functional and design requirements for all aspects of safety related I&C systems. HFC has applied these requirements in the development of the HFC-6000 system. NUREG-0800, references this RG as necessary acceptance criteria. Details regarding compliance with IEEE Std 603 are discussed below.

RG 1.168 Revised 2004 “Verification, Validation, Reviews, and Audits for Digital Computer Software Used In Safety Systems of Nuclear Power Plants”

The HFC V&V process addresses phases of the software life cycle as provided in BTP 7-14 up through the testing and installation of plant specific applications. The life cycle phases for plant operation will be provided during actual plant specific implementation. HFC has documented an acceptable software development methodology and follows this methodology consistently in developing any safety related new software.

[

]

RG 1.169 1997 “Configuration Management Plans for Digital Computer Software
Used In Safety Systems of Nuclear Power Plants”

The HFC’s Software Configuration Management, SCM, Plan documents the requirements, methods and procedures it will use to assure the continued quality of the HFC-6000 platform’s software including both the pre-developed and new software. This plan was formulated based upon the guidance provided by IEEE Std 828 and 1042. The intent of the latter document is to describe an acceptable SCM plan and its implementation. The HFC SCM is applied to all HFC-6000 software and associated documentation including the tools that are used during the design and implementation process.

Guidance and regulations require that the HF-6000 SCM activity be extended to encompass plant specific applications. In order to control and facilitate development of plant specific application efforts, as the HFC platform is fitted to the needs of a specific plant, the SCM will be extended to plant specific configuration activities as described in the HFC’s platform’s life cycle process. The plant specific effort will document the configuration baselines. Any changes to the HFC-6000 digital platform caused by the specific application will be subject to HFC’s SCM stringent change control process.

RG 1.170 1997 “Software Test Documentation for Digital Computer Software
Used In Safety Systems of Nuclear Power Plants”

The HFC-6000 test plan includes the following items: [

]

Additional details are provided in Section 10 of this TR.

RG 1.171 1997 “Software Unit Testing for Digital Computer Software Used In Safety Systems of Nuclear Power Plants”

HFC’s software test methods and procedures, tests conform to the guidance contained in this RG. The tests were performed and the results met all test objectives within the pre-established criteria for the new software. The software performed as specified by the design documents, the interfaces executed as anticipated.

Additional details are provided in Section 10 of this TR.

RG 1.172 1997 “Software Requirements Specifications for Digital Computer Software Used In Safety Systems of Nuclear Power Plants”

The SRS has been written to follow both the guidance contained in this RG and in the endorsed IEEE Std 830. HFC has developed its SRS to address the criteria and guidance of Section 2 of the RG.]

]An SRS

change control program has been implemented by HFC as part of the overall HFC-6000 configuration management program.

The overall SRS conforms to guidance and criteria of the Regulatory Guide and IEEE Std 830. The HFC-6000 SRS are consistent with GDC 1 and the Appendix B criteria for quality assurance programs as they apply to the development of software requirements specifications.

RG 1.173 1997 “Development Software Life Cycle Processes for Digital Computer Software Used In Safety Systems of Nuclear Power Plants”

The RG, BTP 7-14 and the IEEE Std 1074 provide a structured approach for the development of a software life cycle program consistent with regulatory guidance. HFC recognizes that, for development and maintenance of high functional reliability and high quality safety software, there has to be an orderly structure to the entire software design and implementation process. HFC’s Software Life Cycle addresses the issues and concerns of the standard although its

organization differs. The Software Life Cycle process that HFC used successfully provided the necessary framework for the HFC-6000 software project so that activities could be mapped. With this mapping, a concurrent execution of related activities can occur and staged checkpoints are available at which characteristics of certain activities can be verified.

HFC's life cycle plan insures that all necessary development and V&V activities are performed and that the required inputs, outputs, activities, pre-conditions and post-conditions are either described or have been accounted for in the HFC-6000 platform life cycle model. While the RG and IEEE Std do not specify the completion of specific documents, SRP BTP 7-14 places a great degree of emphasis on the output documents as a manner to judge successful completion of a life cycle process. HFC has completed the non-plant specific output documents and provided these to the NRC

RG 1.180 Rev 1 2003 "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems"

The HFC-6000 platform has been tested and evaluated for EMI/RFI based on guidance in this RG and in the EPRI TR on EMC. Details regarding this qualification are discussed in Section 9 of this report.

RG 1.204 2008 Lightning Protection

Plant specific applications should follow the guidance presented in RG 1.204.

RG 1.206 2007 Combined License Applications-summary of guides etc.

HFC has reviewed this RG and noted the guidance and requirements standards that are applicable for the qualification of a safety related digital platform. This report reflects this array of standards and how they relate to the HFC-6000 overall qualification effort.

RG 1.209 2007 Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants

The environmental qualification phase for the HFC-6000 is discussed in more detail in Section 9 of this report and the supplement documents.

NUREG-CR-6303 "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems"

HFC has provided a discussion of its generic concept for meeting Diversity and Defense-in-Depth guidelines as provided in BTP 7-19. This generic discussion is in Section 8-6 of this report. Details regarding this concept will be provided during plant specific implementations.

NUREG-0737 "Requirements for Emergency Response Capability"

The HFC-6000 system will follow the guidance provided by this NUREG. Plant specific implementation descriptions will provide these details.

NUREG-0800 “Standard Review Plan (SRP Chapter 7)” Revised some areas

The design of the HFC-6000 system follows the guidance presented in Chapter 7 of this NUREG that involve I&C digital safety system design. The design and qualification information for both hardware and software is presented in Sections 6 through 10 of this report. Additional details can be found in supporting documentation provided to the NRC and within the HFC library.

NUREG-0800 BTP 7-11 “Guidance for Application and Qualification of Isolation Devices”

[

]

NUREG-0800 BTP 7-14 “Branch Technical Position: Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems”

The HFC software development life cycle considers the guidance provided with this BTP. The HFC new safety related software is developed using software development plans that provide for varied life cycle phases. Management, implementation and resource planning procedures were established for new software. The functional characteristics and software development characteristics noted in the BTP were established and met by the HFC process.

Additional details are provided in Section 10 of this TR.

NUREG-0800 BTP 7-17 “Guidance on Self-Test and Surveillance Test Provisions”

The HFC-6000 is designed for in-service testability of hardware and software components. A balance has been made between providing the self-test capabilities and the added complexity that they introduce. Per the previously described FMEA, HFC surveillance testing and automatic self-testing measures provide adequate mechanisms to detect certain failures.

NUREG-0800 BTP 7-19 “Guidance for Evaluation of Defense-in-Depth and Diversity in Digital-Based I&C Systems”

HFC has provided a generic discussion for meeting Diversity and Defense-in-Depth guidelines in Section 8-6. Detail configurations regarding this concept will be provided during a plant specific implementation.

NUREG-0800 BTP 7-21 “Guidance on Digital Computer Real-Time Performance”

HFC-6000 system timing requirements are such that their allocation to events within a plant's safety analyses should support the timing requirements for each event. This is evident with the use of either small scale or large scale digital system modifications using the HFC-6000. A time analysis for each event will be part of the plant specific implementation process and during the plant specific implementation phase, an acceptable real-time performance will be demonstrated.

8.5.3 Institute of Electrical and Electronic Engineers (IEEE) Standards

IEEE Std 7-4.3.2-2003 “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations”

IEEE 7-4.3.2-2003 provides high-level design criteria for digital computers that includes discussions on qualification of digital systems related to software. The HFC-6000 system design follows the guidance of this RG by meeting the provisions of IEEE-ANS-Std 7-4.3.2. The software for the HFC-6000 is segregated into both pre-developed and new software. For the new safety related software, HFC has described methods employed for designing, verifying, validating and implementing software to be used in safety related systems. The HFC software quality plan is consistent with ASME NQA-2a; this plan addresses all of the runtime resident computer software. The verification and validation processes are in accordance with all applicable guidance. Those processes provide adequate confidence that the safety requirements and the requirements defined at each phase of the development process are implemented. The pre-developed software is qualified based on the provisions of Section 5.3.2 and Appendix D of the IEEE Std standard. Qualification factors were developed per the guidance of EPRI's TR-106439 and TR-107330. The discussion in Section 10 of this report provides the qualification criteria taken from both of these reports and provides a high-level discussion comparing the specific design criteria to the HFC-6000 System design. There is also a reference to other Sections of this report where additional discussion can be found. Other guides and standards are referenced for applicability.

Additional design and licensing criteria discussed in NUREG-0800, “Standard Review Plan (SRP Chapter 7), was also used in the digital platform design. The design of the HFC-6000 system followed guidance presented in Chapter 7 of this NUREG that involve I&C digital safety system design. The design and qualification information for both hardware and software is presented in Sections 6 through 10 of this report. Additional details can be found in supporting documentation within the HFC library of documents. Industry guidance contained in EPRI TR-107330, “Generic Requirements Specifications for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants”, December 1996 was used for setting the qualification criteria for the HFC-6000. Per this standard, a matrix was developed that demonstrates that the HFC-6000 system design process complies with the individual specifications of this guidance document.

[

] If the plant-specific system requirements identify a system preferred failure mode, failures of the HFC-6000 platform would not preclude the safety system from being placed in that mode. HFC has provided a design assuring that test and calibration functions will not adversely affect the ability of the controller to perform its safety function.

The HFC-6000 platform incorporates self-diagnostics functions scheduled for every scan cycle to detect and report system faults and failures in a timely manner. These self-diagnostic functions do not adversely affect the ability of the HFC-6000 platform to perform its designated safety function, or cause any spurious actuations of the safety function.

IEEE Std 323-2003 Revised “IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations

The HFC-6000 was environmentally qualified using the guidance contained in EPRI TR-107330, RG 1.209 and this IEEE Std. This qualification effort is discussed in more detail within Section 9 of this report and supplemental documentation.

IEEE Std 344-1987 Revised “IEEE Standard for Seismic Qualification of Class I Electric Equipment for Nuclear Power Generating Stations”

The HFC-6000 system meets the seismic qualification criteria for safety related equipment. This is discussed in more detail in Section 9 of this report. The seismic test criteria represented the OBEs and SSEs discussed in EPRI TR-107330.

IEEE Std 352-1987 “IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems

The reliability and FMEA of the HFC-6000 system has been analyzed and the results are presented in Section 8 of this report. These results show that this system is highly reliable and acceptable for use in safety related systems. The results of the FMEA show that the HFC-6000

meets acceptance criteria. A plant specific application will provide system reliability and additional FMEA details.

IEEE Std 379-2000 “IEEE Standard Application of Single Failure Criterion to
Nuclear Power Generating Station Class 1E Systems”

The HFC-6000 system meets the single failure requirements of IEEE Std 603 in addition to the guidance contained in this IEEE. However, this is only when the system is installed in a redundant design. When this occurs, considering the single failure criterion in association with all potential HFC-6000 applications, all requisite safety functions can be maintained without impeding the execution of other safety functions. This is valid for all functions where redundancy is maintained. The actual design and review of the HFC-6000 system in meeting the single failure criterion should occur during the plant-specific implementation review.

IEEE Std 384-1977 “Criteria for Independence of Class 1E Equipment and Circuits”

The review to meet the guidance of the IEEE Std should occur during the plant-specific implementation phase. |

IEEE Std 472-1974 “Guide for Surge Withstand Capability Tests”

Surge withstand testing was performed on the HFC-6000 system in accordance with the guidance presented in EPRI TR-107330. Details regarding the test results are presented in Section 9 of this report.

IEEE Std 577-1976 “IEEE Standard Requirements for Reliability Analysis in the
Design and Operation of Safety Systems for Nuclear Power
Generating Stations

See the response to IEEE Std 352-1987.

IEEE Std 603-1991 “IEEE Standard Criteria for Safety Systems for Nuclear Power
Generating Stations”

This IEEE Std establishes functional and design requirements for all aspects of safety related I&C systems. HFC has applied these requirements in the development and qualification of the HFC-6000 system. NUREG-0800 references this IEEE Std as necessary acceptance criteria. RG 1.152, “Criteria for Programmable Digital Computer System Software in Safety-Related Systems of Nuclear Power Plants” provides software guidance that supplements this IEEE Std. RG 1.153 “Criteria for Safety Systems” endorses IEEE Std 603.

Additional design and licensing criteria discussed in NUREG-0800, “Standard Review Plan (SRP Chapter 7), were also used in the digital platform design. The design of the HFC-6000

system followed guidance presented in Chapter 7 of this NUREG involving I&C digital safety system design. The design and qualification information for both hardware and software is presented in Sections 6 through 10 of this report. Additional details can be found in supporting documentation within the HFC library. Industry guidance contained in EPRI TR-107330, "Generic Requirements Specifications for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants, December 1996" was used for setting up the qualification criteria for the HFC-6000 digital platform. Per this standard, a matrix was developed that demonstrates that the HFC-6000 system design complies with the individual specifications of this guidance document. Individual IEEE Std 603 safety system criteria are discussed below.

Single-Failure Criterion:

The results of the FMEA report show that there are no undetectable failures that affect any HFC-6000 safety function. While the HFC-6000 has significant redundancy there are certain single failures that will defeat the operational capability of the digital platform. However, plant specific applications will implement the HFC-6000 in redundant systems such that the Single Failure Criterion will be met.

Completion of Protective Action:

The completion of the protective action review should be carried out during the plant specific implementation phase when the channel outputs are distributed to the corresponding logic.

Quality:

The HFC-6000 hardware conforms to the quality assurance provisions of 10 CFR Part 50 Appendix B as well as NQA1-1989. The software quality requirements of IEEE Std 7-4.3.2 are met by the HFC software quality program which is implemented in two separate sections. The first section is the pre-developed software whose quality is assured through the HFC pre-developed software program. This program is discussed in Section 10 of this report. This program consists of a large operational data base accrued since 1990; a reverse-engineered review process to determine software quality; and an application of current quality guidance. The second section is the new software (application specific software) which is developed under a program that meets current requirements and guidance.

Equipment Qualification:

The HFC-6000 equipment has been qualified in accordance with the guidance contained in EPRI TR-107330, IEEE Std 323-1987/2003, IEEE 344-1987, RG 1.180 Rev 1 and EPRI TR-102323-R1. RG 1.180 Rev 1 and EPRI TR-102323-R1 were used as guidance for EMC qualification. This is discussed in detail in Section 9 of this report.

System Integrity:

The HFC-6000 system design includes the qualification of equipment for the condition that should be specified in a plant-specific design basis. This is assured by the conservative design of the HFC-6000 as verified during the equipment qualification testing as discussed in Section 9 of this TR. However, the plant-specific boundaries would need to be affirmed before actual

implementation could proceed. Another integrity concern is the timing for signal processing. The HFC individual controller timing has been verified but would need to be bounded by plant specific analyses for each postulated event.

Independence:

[

]

Capability for Test and Calibration:

The HFC-6000 system is designed to meet the guidance of RG 1.22, RG 1.118, and IEEE Std 338-1987. The extent of the inherent test and calibration features including the on-line testing capability provide assurance that the single failure criterion is met and automatic operability is confirmed. Data errors and computer lockup are detected by plant specific and diagnostic test provisions. Disconnecting wires, installing jumpers or other similar modifications are not necessary to perform the requisite testing.

Information Displays:

There are only operability lights associated with the HFC-6000 system. There is no data information displays associated with the HFC-6000 system.

Control of Access:

The HFC-6000 has several design features to provide means to control the physical access including access to test points for verifying and changing. Plant specific implementation will provide additional details for safety system doors and control of access to rooms and equipment.

Repair:

The HFC-6000 has on-line diagnostics to aid in troubleshooting as well as periodic on-line/off-line surveillance procedures such as calibrations and functional testing. With modular components, repairs are done in a rapid fashion.

Identification:

The identification of hardware components is controlled by HFC with its numbering system and record keeping capabilities. This is part of the HFC Configuration Management Plan. Coding of cabinets and cabling is a plant-specific item.

Auxiliary Features:

Not applicable for this Topical Report.

Multi-unit Stations:

Not applicable for this Topical Report.

Human Factor Considerations:

Equipment performance indicators and calibration processes are designed to conform to current human factor criteria. Additional human factor considerations will be coordinated and consistent with a licensee's commitments as documented in Chapter 18 of the UFSAR. This will be affirmed during the plant specific implementation.

Reliability:

Reliability and Quality of the HFC-6000 system is discussed in several sections of the TR. Redundancy, diversity and testability which adds to reliability will be addressed during the plant specific implementation phase.

Automatic Control:

The HFC-6000 design meets this requirement by providing the capability to automatically actuate and control protective actions. The actual implementation will occur during the plant specific implementation phase.

Manual Control:

The HFC-6000 design meets this requirement by providing the capability to manually actuate and control protective actions. The actual manual implementation design will occur during the plant specific implementation phase.

Interaction Between the Sense and Command Features and Other Systems:

[

]

Deviation of System Inputs:

The deviation of system inputs is part of the plant specific design.

Operating and Maintenance Bypass:

Operating and Maintenance Bypass is part of the plant specific design.

Setpoints:

The HFC-6000 system is designed such that the setpoints for nuclear plants can be maintained considering anticipated operating transient and postulated accident conditions. Measurement uncertainties will be considered and factored into a plant's setpoint methodology. The actual plant setpoint methodology will be provided during the plant specific implementation phase.

IEEE Std 730-1989

“Software Quality Assurance Plans”

The HFC-6000 system quality assurance plans conform to the guidance of this Std. A discussion of the QA process is presented in Section 8 of this report. Supporting information is provided in HFC Quality Process Procedures and HFC Quality Plans. HFC's software quality assurance plan is compliant with this standard as well as 10 CFR Part 50 Appendix B.

IEEE Std 828-1990 “IEEE Standard for Software Configuration Management Plans
(ANSI)

The software configuration management plans for HFC-6000 are discussed in the response to RG 1.169 above.

IEEE Std 829-1983 “IEEE Standard for Software Test Documentation”

See the RG 1.170 discussion above.

IEEE Std 830-1984 “IEEE Standard Guide for Software Requirements
Specification”

See the RG 1.172 discussion above.

IEEE Std 1008-1987 “IEEE Standard for Software Unit Testing”

See the RG 1.171 discussion above.

IEEE Std 1012-1998 “IEEE Standard for Software Verification and Validation
Plans”

The HFC-6000 system verification and validation plans conform to this standard as described in the HFC software design descriptions and as noted in the RG 1.168 discussion above. This is applicable for all new software including all application software.

IEEE Std 1016-1987 “Recommended Practice for Software Design Description”

The HFC software design (both new and pre-developed software) offers the necessary information content and organization for a software design description that follows the guidance of both IEEE Stds 1016 and 1016.1. HFC recognized early on that a software design that was easily reviewed and understood by all interested parties would facilitate the acceptance of the system by designers, regulators and end-users alike. The resulting HFC-6000 Software Design Description is extremely “viewable” with descriptions of all categories of component software including clear descriptions of its purpose and discussions of its other salient attributes.

IEEE Std 1028-1988 “Standard for Software Reviews and Audits”

HFC complies with this Std. The HFC-6000 Quality Assurance Program assures that the requisite software reviews and audits are performed.

IEEE Std 1042 “IEEE Guide to Software Configuration Management”

The Software Configuration Management program for the HFC-6000 is discussed later in this report (Section 10) and also addressed in the RG 1.169 discussion above.

IEEE Std 1074-1995 “IEEE Standard for Developing Software Life Cycle Processes”

A life cycle is established for the design of any new software for the HFC-6000 system. This includes all application software. See the RG 1.173 discussion above and also the discussion on this topic in Section 10 of this TR.

IEEE Std 1228-1994 “IEEE Standard for Software Safety Plans”

The HFC-6000 system design includes the aspects of software safety management, software safety analyses, and post development which include training, installation, startup and transition, operations support, monitoring maintenance, and retirement. The HFC organization, schedule, resources, responsibilities, tools, techniques and methodologies used in the development of the safety related software were included in these aspects. As part of the software development process, an analysis was continually performed on the requirements, preparation, designing, coding and testing. Training, monitoring, maintenance, event analyses and retirement are necessary issues that will be addressed during plant specific implementation.

IEEE Std C37.90.1-1989 “IEEE Standard Surge Withstand Capability (SWC) Tests for Protective Relays and Relay Systems (ANSI)”

Surge withstand capability was part of the electrical qualification tests for the HFC-6000 system. This is discussed in detail in the test reports and also in Section 9 of this report as well as supplemental documentation.

8.5.4 Other Documents

ISA S67-06-1984 “Response Time Testing on Nuclear Safety-Related Instrumentation Channels”

The response time of the HFC-6000 system has been verified to be within acceptable limits for a generic set of safety-related plant specific applications. Of course, for each plant specific application this response time will be re-verified during both factory and site acceptance testing.

ISA S67-04 Part I-1994 “Setpoints for the Nuclear Safety-Related Instrumentation”

The HFC-6000 system is designed such that the setpoints for nuclear plants can be maintained considering anticipated operating transient and postulated accident conditions. Measurement uncertainties will be considered and easily factored into a plant’s setpoint methodology. The actual setpoint methodology will be provided during a plant specific implementation.

MIL-STD-461C “Requirements for the Control of Electromagnetic Interference Emissions and Susceptibility”

The HFC-6000 system was tested for EMI/RFI in accordance with RG 1.180 Rev. 1 and EPRI-TR102323-R1. This testing and the test results demonstrated that per this standard, the HFC-

6000 is qualified for safety related applications. Testing details and results are provided in Section 9 of this report.

MIL-STD-462D-461E “Measurement of Electromagnetic Interference Characteristics”

The HFC-6000 system was tested for EMI/RFI in accordance with RG 1.180 Rev. 1 and EPRI-TR102323-R1. This testing and the test results show that it is qualified for safety related applications. Test procedures were established that follow the guidance of this MIL-STD. Testing details are provided in Section 9 of this report.

ASME NQA-1/NQA-2 “QA of Design Software”

The HFC quality assurance processes follow the guidance presented in these ASME standards and also meet the requirements of 10 CFR 50 Appendix B. Section 8 of this report provides a summary of the quality assurance process for the HFC-6000 system. Additional details are provided in HFC supporting documents.

EPRI TR-102323-R1 “Guidelines for Electromagnetic Interference Testing in Power Plants, April 30, 1996”

The HFC-6000 system was tested for EMI/RFI in accordance with EPRI-TR102323-R1. The results demonstrate that the HFC-6000 is qualified for safety related applications. EMI/RFI testing and test results can be found in Section 9 of this report.

EPRI TR-102348 “Guideline on Licensing Digital Upgrades; December 1993”

The applicable portions of this EPRI document were followed during the finalization of the design process of the HFC-6000 system. A significant portion of the document’s guidance concerns plant specific concerns. Therefore, guidance in this area will be applied and conformed to during plant specific applications.

EPRI TR-103291 “Handbook of Verification and Validation for Digital Systems, Vol. 1: Summary, Vol. 2: Case Histories, Vol. 3: Topical Reviews, December 1994”

The verification and validation process used for the new software followed the guidance contained in IEEE Std 1012 and IEEE-ANS Std 7-4.3.2. This EPRI document was used to the extent necessary to reflect and apply the IEEE Std guidance and for additional knowledge and lessons learned.

EPRI-TR 106439 “Guidelines on evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications”

The HFC-6000 digital platform operational system uses commercial grade software that is designated in this report as pre-developed or legacy software. To ensure a level of adequacy for

this software commensurate with 10 CFR Part 50 Appendix B, the guidance provided in this TR was used extensively by HFC. The layered approach as illustrated in Figure 10-2 of the TR was used by HFC as the process for dedication of the HFC-6000 pre-developed software (PDS). Details regarding this process are discussed in Section 10 of this report, supporting documents provided to the NRC and in the library of HFC supporting documentation.

EPRI TR-107330

“Generic Requirements Specifications for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants, December 1996”

This EPRI TR provides generic specifications and requirements for qualifying commercially available PLCs for application in safety-related I&C systems at nuclear power plants. HFC used these generic specifications and requirements to qualify the HFC-6000 digital platform. These specifications are suitable for evaluating a digital platform like the HFC-6000, establishing a suitable qualification test program, and confirming that the quality assurance program is adequate for safety-related applications. The specifications include requirements for detailed design characteristics, quality assurance measures, documentation to support this qualification and the documentation to support plant specific implementation. Per this standard, a matrix was developed that demonstrates that the HFC-6000 system design complies with the individual specifications of this guidance document.

8.5.5 CFR and General Design Criteria (GDC)

a) GDC 1 - Quality Standards And Records (Category A)

The HFC-6000 QA procedures and record-keeping both conform to this requirement. Details are provided in Section 8 of this report and HFC supporting documentation.

b) GDC 2 - Design Bases For Protection Against Natural Phenomena (Category A)

The HFC-6000 system has been tested and found to conform to the requisite seismic design criteria. Details are provided in Section 9 of this report.

c) GDC 4 - Environmental And Missile Design Bases

The design basis for this requirement has been met and proven via qualification testing of the HFC- 6000 system. Details are provided in Section 9 of this report and HFC supporting documentation. Plant specific implementation will provide further information and should be reviewed at that time.

d) GDC 13 - Instrumentation And Control

The HFC-6000 is designed and tested to this requirement.

e) GDC 19 - Control Room

The control room requirements of this GDC are supported by the HFC-6000 design. Actual plant specific implementation will provide the control room design details. The requirements for an auxiliary shutdown location will be discussed during a plant specific implementation.

f) GDC 20 - Protection System Functions

The HFC-6000 has been designed for automatic initiation capabilities such that fuel design limits should not be exceeded for both transients and accidents. The requirements of this GDC are met by the margins included in the design and will be verified by proof testing. Actual plant specific implementation will provide the design details for this area.

g) GDC 21 - Protection System Reliability And Testability

The reliability and testability of the HFC-6000 digital platform meets the requirements of this GDC and is discussed in more detail in later sections of this TR.

h) GDC 22 - Protection System Independence

Protection system independence for the HFC-6000 based safety systems meets the requirements of this GDC.]

]This is discussed in more detail in Section 8.9 of this TR. Actual plant specific implementation will provide a plant-wide system level independence design that should be reviewed at that time.

i) GDC 23 - Protection System Failure Modes

HFC-6000 plant specific protection systems are designed (and verified) to fail to a fail-safe or acceptable state. For the Reactor Trip System for a plant-specific design, the loss of power will cause a reactor trip and for the Engineered Safety Features, the loss of power will cause the system to fail as is. A plant specific review is necessary to provide the determination of this feature at the system level.

j) GDC 24 - Separation of Protection And Control Systems

The HFC-6000 system design ensures that there is adequate separation of protection and control systems per this criterion. The HFC-6000 digital platform has connections to non-safety related equipment via the C-Link.]

] k) GDC 25 - Protection System Requirements for Reactivity Control Malfunctions

The HFC-6000 reactivity control systems will meet the requirements of this GDC. The review for this criterion is part of the plant specific implementation review.

l) GDC 29 - Protection Against Anticipated Operational Occurrences

HFC-6000 based protection and reactivity control systems will continue to meet the requirements of this GDC. Failure to accomplish the safety function has been determined to be unlikely. However, details are part of the plant specific implementation review.

m) GDC 37 - Testing of Emergency Core Cooling System

ESFAS HFC-6000 system applications will support this requirement with its configurations for periodic and functional testing. However, details are part of the plant specific implementation review.

n) GDC 40 - Testing of Containment Heat Removal System

o) GDC 43 - Testing of Containment Atmosphere Cleanup Systems

p) GDC 46 - Testing of Cooling Water System

q) GDC 54 - Systems Penetrating Containment

The above four GDC's are supported by the HFC-6000 system design when it is used in plant specific applications as called for by the individual criterion. However, details are part of the plant specific implementation review.

r) 10 CFR Part 50, Appendix B

All activities affecting the safety related functions of the HFC-6000 system meet the requirements of this Appendix and have been audited by a NUPIC member. The requirements of Appendix B are rigorously adhered to during the design control process, purchasing, fabricating, handling, shipping, storing, building, inspecting, testing, operating, maintaining, repairing and modifying of the HFC-6000 system. Quality assurance for the HFC-6000 system consists of the proper planned and systematic actions necessary to provide adequate confidence that that the HFC-6000 system will perform as required. Additional details regarding quality assurance activities for the HFC-6000 system are discussed in this section and are available for staff review and audit. Supplemental QA documentation contains further information.

s) 10 CFR Part 21

HFC, as the manufacturer for the HFC-6000 system, is responsible for adhering to requirements of Part 21.

t) 10 CFR Part 50.36

The HFC-6000 design will be able to maintain plant specific required limiting safety system settings. The HFC-6000 system setpoint methodology will readily replace existing analog system

setpoint methodologies with an accuracy and drift control rate superior to that previously reported with analog systems. This will be demonstrated during a plant specific implementation phase.

u) 10 CFR Part 50.49

The HFC-6000 is environmentally qualified for a mild environment in accordance with the guidance of IEEE Std 323 and RG 1.209. The qualification process is described in more detail in association with the discussion of the system's compliance with the qualification criteria presented in EPRI TR-107330. This discussion can be found in Section 9 of this report.

v) 10 CFR Part 50.62

This requirement is only relevant upon a plant specific implementation of the HFC-6000.

8.6 Defense-in-Depth and Diversity Evaluation Process

8.6.1 NRC Position 1

The applicant/licensee should assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-mode failure have been adequately addressed.

8.6.1.1 Compliance to Position 1

A plant specific diversity and defense-in depth analysis will be performed utilizing the guidelines provided in NUREG/CR 6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," December 1994. In addition, newly available guidance in the Draft Interim Staff Position on D3 will be used during a plant specific implementation.

The analysis will demonstrate that diverse plant equipment and operator action can be utilized to cope with the plant's design basis anticipated operational occurrences concurrent with a common-mode failure in the HFC-6000 software-based equipment, such that the acceptance criteria stated in BTP 7-19 will be met. The defense-in-depth and diversity analysis will utilize best-estimate analytical methods and realistic assumptions, including crediting operator action where adequate displays and controls remain that are not affected by the common-mode failure and sufficient time exists to perform the operator action.

8.6.2 NRC Position 2

In performing the assessment, the vendor or applicant/licensee shall analyze each postulated common-mode failure for each event that is evaluated in the accident analysis section of the

safety analysis report (SAR) using best-estimate methods. The vendor or applicant/licensee shall demonstrate adequate diversity within the design for each of these events.

8.6.2.1 Compliance to Position 2

To simplify the defense-in-depth and diversity analysis, postulated common-mode failures of the software-based HFC-6000 equipment will be assumed to occur in such a manner that safety functions performed in this equipment will be disabled. The defense-in-depth and diversity analysis will then assume that the remaining plant instrumentation and control systems that do not utilize the HFC-6000 software-based equipment are available to be utilized to cope with the plant's design basis anticipated operational occurrences. This analysis will be performed on a plant specific base at a later date.

8.6.3 NRC Position 3

If a postulated common-mode failure 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 common-mode failure, should be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.

8.6.3.1 Compliance to Position 3

The defense in depth and diversity analysis will consider each plant specific design basis anticipated operational occurrence that is evaluated in the plant's UFSAR. For each anticipated operational occurrence, a postulated common-mode failure in the software-based HFC equipment will be assumed in such a manner that the safety functions performed by the equipment are disabled. The analysis will then utilize the remaining diverse plant instrumentation and control systems and credit operator actions that are based on displays, indication, and alarms that are not affected by the common mode failure. The credit for operator action will utilize realistic assumptions for the time required to diagnose the plant transient and perform the required actions. The HFC-6000 safety system will be configured to enhance the plant's defense- in depth and diversity. Specific design techniques that will be utilized are described below.

8.6.4 Critical Analog Signals

Critical analog signals are defined as those signals that are utilized as input signals to the HFC-6000 safety system and that are also required to be utilized for indicator and/or control functions that support the defense-in depth and diversity analysis. For these signals, a separate analog signal(s) will be developed prior to the utilization of the signal in the HFC-6000 safety system as shown in the example in Figure 8-1 below. The separate analog signal will be isolated with a class 1E qualified isolator and sent to indicators and/or control system outside the safety channel.

In the event that only an indication is required to support an operator action, the diverse control system or operator action based on the control device could be credited in the defense-in-depth and diversity analysis to assist in coping with the anticipated operation occurrence.

[

]

Figure 8-1 - Configuration for Critical Analog Signals

8.6.5 Critical Manual Signals

Critical manual signals are defined as manual control signals that are utilized to initiate a safety system function or to control a safety system component in the diversity and defense-in-depth analysis. These manual control inputs are typically system-level manual actuations of reactor trip or manual actuation of a specific engineered safety feature. These critical manual signals will be implemented in a manner that assures that they are independent of the HFC-6000 software-based safety functions.

8.6.6 Implementation of Critical Manual Signals

For reactor trip, the manual actuation signal will be implemented downstream of the HFC-6000 software-based automatic reactor trip functions. For engineered safety features actuation, the manual actuation will be implemented downstream of the automatic software-based engineered safety features action output.

8.6.7 Conclusion

The HFC concept for safety is based upon a simple system approach. Quality is designed and built into the HFC-6000 system such that any type of failure both hardware and software is highly unlikely. The design, qualification, and in-service testing afforded by the HFC-6000 system are implemented to minimize the probability of failures of all types. However, additional

safety is achieved by employing the concepts of defense-in-depth and diversity. HFC's strategy for Diversity and Defense-In-Depth techniques has been devised to satisfy NRC acceptance criteria contained in BTP 7-19. The HFC goal is to meet the requirements with the following implementation goals:

- New diverse instrumentation and manual controls should be limited because of the manner in which the HFC-6000 is designed and implemented at plant sites. The existing information available will be retained such that the plant can be placed in a hot-shutdown condition concurrent with a postulated SWCMF to the HFC-6000.
- Engineering assessments will be acceptable for most of FSAR Chapter 15 accident analysis. A detailed quantitative assessment will not be necessary. Where possible, risk-based assessments will be used to determine the significance of the event concurrent with the postulated SWCMF. This risk-based effort will follow the guidance offered by EPRI and the NRC.

The HFC-6000 architecture has been carefully designed and analyzed using the concepts and guidance of NUREG/CR-6303 and BTP 7-19 to assure that the plant control systems, AMSAC, and indications necessary for operator action remain available and are not subject to the postulated SWCMF. As stated above, the HFC design which includes measures for error avoidance and fault tolerance are extremely effective at both preventing and minimizing the consequences of postulated software failures.

HFC has demonstrated and will be able to demonstrate for future plant specific applications that the HFC-6000 design addresses Diversity and Defense-in-Depth consistent with NRC requirements and satisfy NRC acceptance criteria for this topic. Furthermore, HFC and future plant specific customers are expected to follow the risk-based Defense-in-Depth and Diversity assessment guidance and will use it when NRC approval is granted. Implementation of plant-specific HFC-6000 Instrumentation and Control system upgrades in accordance with guidance offered in NUREG/CR-6303 and BTP 7-19 assures that adequate diversity and defense-in-depth is provided with HFC's design approach.

8.7 Cyber Security

To adequately protect the HFC-6000 safety system from cyber security based intrusions and faults, a secure design including administrative requirements has been implemented by HFC.

[

8.8 Isolation and Independence

The HFC-6000 platform is qualified as a safety related device without any non-safety related components. However, the C-Link does provide for the capability of communication to other controllers within one division (intra division) and for one-way communication to non-safety related components[

]However, these connections could be provided during a plant specific implementation phase. The actual details for acceptable isolation and independence for these areas will be provided during this plant specific implementation phase.

8.9 Digital Instrumentation and Controls (DI&C) Interim Staff Guidance (ISG)-04, Communications Issues

The C-Link provides intra-divisional communication capability that includes the transmission of data and information within an electrical safety division and communications between safety related controllers and non-safety related equipment. The C-Link intra-divisional communication capabilities are bi-directional within the same division and unidirectional to non-safety related equipment.

The NRC has stated that bi-directional communications within a safety division and one way communication between safety and non-safety related equipment is acceptable provided certain restrictions are enforced to ensure that there will be no adverse impact on safety systems. Design guidance for acceptance is provided in ISG-04 on communications issues. The C-Link of the HFC-6000 adheres to this ISG on communication as discussed below. The ISG-04 guidance is discussed (*Italics*) in the initial paragraph of each item.

1. A safety channel should not be dependent upon any information or resource originating or residing outside its own safety division to accomplish its safety function. This is a fundamental consequence of the independence requirements of IEEE603. It is recognized that division-voting logic must receive inputs from multiple safety divisions.

[

]

2. The safety function of each safety channel should be protected from adverse influence from outside the division of which that channel is a member. Information and signals originating outside the division must not be able to inhibit or delay the safety function. This protection must be implemented within the affected division (rather than in the sources outside the division), and must not itself be affected by any condition or information from outside the affected division. This protection must be sustained despite any operation, malfunction, design error, communication error, or software error or corruption existing or originating outside the division.

[

]

3. A safety channel should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function.

Receipt of information that does not support or enhance the safety function would involve the performance of functions that are not directly related to the safety function. Safety systems should be as simple as possible. Functions those are not necessary for safety, even if they enhance reliability, should be executed outside the safety system. A safety system designed to perform functions not directly related to the safety function would be more complex than a system that performs the same safety function, but is not designed to perform other functions. The more complex system would increase the likelihood of failures and software errors. Such a complex design, therefore, should be avoided within the safety system. For example, comparison of readings from sensors in different divisions may provide useful information concerning the behavior of the sensors (for example, On-Line Monitoring). Such a function executed within a safety system, however, could also result in unacceptable influence of one division over another, or could involve functions not directly related to the safety functions, and should not be executed within the safety system. Receipt of information from outside the division, and the performance of functions not directly related to the safety function, if used, should be justified. It should be demonstrated that the added system/software complexity associated with the performance of functions not directly related to the safety function and with the receipt of information in support of those functions does not significantly increase the likelihood of software specification or coding errors, including errors that would affect more than one division. The applicant should justify the definition of "significantly" used in the demonstration.

[

]

4. The communication process itself should be carried out by a communications processor separate from the processor that executes the safety function, so that communications errors and malfunctions will not interfere with the execution of the safety function. The communication and function processors should operate asynchronously, sharing information only by means of dual-ported memory or some other shared memory resource that is dedicated exclusively to this exchange of information. The function processor, the communications processor, and the shared memory, along with all supporting circuits and software, are all considered to be safety-related, and must be designed, qualified, fabricated, etc., in accordance with 10 C.F.R. Part 50, Appendix A and B. Access to the shared memory should be controlled in such a manner that the function processor has priority access to the shared memory to complete the safety function in a deterministic manner. For example, if the communication processor is accessing the shared memory at a time when the function processor needs to access it, the function processor should gain access within a timeframe that does not impact the loop cycle time assumed in the plant safety analyses. If the shared memory cannot support unrestricted simultaneous access by both processors, then the access controls should be configured such that the function processor always has precedence. The safety function circuits and program logic should ensure that the safety function will be performed within

the timeframe established in the safety analysis, and will be completed successfully without data from the shared memory in the event that the function processor is unable to gain access to the shared memory.

[

]

Figure 8-2 – Public Memory shared between C-Link and SYS processors

5. The cycle time for the safety function processor should be determined in consideration of the longest possible completion time for each access to the shared memory. This longest-possible completion time should include the response time of the memory itself and of the circuits associated with it, and should also include the longest possible delay in access to

the memory by the function processor assuming worst-case conditions for the transfer of access from the communications processor to the function processor. Failure of the system to meet the limiting cycle time should be detected and alarmed.

[

]

6. The safety function processor should perform no communication handshaking and should not accept interrupts from outside its own safety division.

[

]

7. Only predefined data sets should be used by the receiving system. Unrecognized messages and data should be identified and dispositional by the receiving system in accordance with the pre-specified design requirements. Data from unrecognized messages must not be used within the safety logic executed by the safety function processor. Message format and protocol should be pre-determined. Every message should have the same message field structure and sequence, including message identification, status information, data bits, etc. in the same locations in every message. Every datum should be included in every transmit cycle, whether it has changed since the previous transmission or not, to ensure deterministic system behavior.

[

]

8. Data exchanged between redundant safety divisions or between safety and no safety divisions should be processed in a manner that does not adversely affect the safety function of the sending divisions, the receiving divisions, or any other independent divisions.

[

]
9. *Incoming message data should be stored in fixed predetermined locations in the shared memory and in the memory associated with the function processor. These memory locations should not be used for any other purpose. The memory locations should be allocated such that input data and output data are segregated from each other in separate memory devices or in separate pre-specified physical areas within a memory device.*
[

]
Table 8-1 - Software Layers of C-Link processor
[

]

10. *Safety division software should be protected from alteration while the safety division is in operation. On-line changes to safety system software should be prevented by hardwired interlocks or by physical disconnection of maintenance and monitoring equipment. A workstation (e.g. engineer or programmer station) may alter addressable constants, setpoints, parameters, and other settings associated with a safety function only by way of the dual-processor / shared-memory scheme described in this guidance, or when the associated channel is inoperable. Such a workstation should be physically restricted from making changes in more than one division at a time. The restriction should be by means of physical cable disconnect, or by means of key-lock switch that either physically opens the data transmission circuit or interrupts the connection by means of hardwired logic. "Hardwired logic" as used here refers to circuitry that physically interrupts the flow of information, such as an electronic AND gate circuit (that does not use software or firmware) with one input controlled by the hardware switch and the other connected to the information source: the information appears at the output of the gate only when the switch is in a position that applies a "TRUE" or "1" at the input to which it is connected. Provisions that rely on software to effect the disconnection are not acceptable. It is noted that software may be used in the safety system or in the workstation to accommodate the effects of the open circuit or for status logging or other purposes.*

[

11. *Provisions for interdivisional communication should explicitly preclude the ability to send software instructions to a safety function processor unless all safety functions associated with that processor are either bypassed or otherwise not in service. The progress of a safety function processor through its instruction sequence should not be affected by any message from outside its division. For example, a received message should not be able to direct the processor to execute a subroutine or branch to a new instruction sequence.*

[

12. *Communication faults should not adversely affect the performance of required safety functions in any way. Faults, including communication faults, originating in non-safety*

equipment, do not constitute "single failures" as described in the single failure criterion of 10 C.F.R. Part 50, Appendix A. Examples of credible communication faults include, but are not limited to, the following:

- Messages may be corrupted due to errors in communications processors, errors introduced in buffer interfaces, errors introduced in the transmission media, or from interference or electrical noise.
- Messages may be repeated at an incorrect point in time.
- Messages may be sent in the incorrect sequence.
- Messages may be lost, which includes both failures to receive an uncorrupted message or to acknowledge receipt of a message.
- Messages may be delayed beyond their permitted arrival time window for several reasons, including errors in the transmission medium, congested transmission lines, interference, or by delay in sending buffered messages.
- Messages may be inserted into the communication medium from unexpected or unknown sources.
- Messages may be sent to the wrong destination, which could treat the message as a valid message.
- Messages may be longer than the receiving buffer, resulting in buffer overflow and memory corruption.
- Messages may contain data that is outside the expected range. Messages may appear valid, but data may be placed in incorrect locations within the message.
- Messages may occur at a high rate that degrades or causes the system to fail (i.e., broadcast storm).
- Message headers or addresses may be corrupted.

[

13. Vital communications, such as the sharing of channel trip decisions for the purpose of voting, should include provisions for ensuring that received messages are correct and are correctly understood. Such communications should employ error-detecting or error-correcting coding along with means for dealing with corrupt, invalid, untimely or otherwise questionable data. The effectiveness of error detection/correction should be demonstrated in the design and proof testing of the associated codes, but once demonstrated is not subject to periodic testing. Error-correcting methods, if used, should be shown to always reconstruct the original message exactly or to designate the message as unrecoverable. None of this activity should affect the operation of the safety-function processor.

[

]

14. Vital communications should be point-to-point by means of a dedicated medium (copper or optical cable). In this context, "point-to-point" means that the message is passed directly from the sending node to the receiving node without the involvement of equipment outside the division of the sending or receiving node. Implementation of other communication strategies should provide the same reliability and should be justified.

[

]

15. Communication for safety functions should communicate a fixed set of data (called the "state") at regular intervals, whether data in the set has changed or not.

[

]

16. Network connectivity, liveness, and real-time properties essential to the safety application should be verified in the protocol. Liveness, in particular, is taken to mean that no connection to any network outside the division can cause an RPS/ESFAS communication protocol to stall, either deadlock or livelock. (Note: This is also required by the independence

criteria of: (1) 10 C.F.R. Part 50, Appendix A, General Design Criteria ("GDC") 24, which states, "interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired."; and (2) IEEE 603-1991 IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.) (Source: NUREG/CR-6082, 3.4.3).

|

]

17. Pursuant to 10 C.F.R. § 50.49, the medium used in a vital communications channel should be qualified for the anticipated normal and post-accident environments. For example, some optical fibers and components may be subject to gradual degradation as a result of prolonged exposure to radiation or to heat. In addition, new digital systems may need susceptibility testing for EMI/RFI and power surges, if the environments are significant to the equipment being qualified.

|

]

18. Provisions for communications should be analyzed for hazards and performance deficits posed by unneeded functionality and complication.

The C-Link has been analyzed for hazards and performance deficits as part of the digital platform FMEA. The results of this analysis are provided in the HFC-6000 FMEA.

19. If data rates exceed the capacity of a communications link or the ability of nodes to handle traffic, the system will suffer congestion. All links and nodes should have sufficient capacity to support all functions. The applicant should identify the true data rate, including overhead, to ensure that communication bandwidth is sufficient to ensure proper performance of all safety functions. Communications throughput thresholds and safety system sensitivity to communications throughput issues should be confirmed by testing.

|

]
20. The safety system response time calculations should assume a data error rate that is greater than or equal to the design basis error rate and is supported by the error rate observed in design and qualification testing.
[

]

9 Equipment Qualification

9.1 Introduction

HFC has completed the equipment qualification of the HFC-6000 system for safety-related applications in U. S. nuclear power plants. This section identifies the specific combination of tests that were performed, summarizes the results, and presents the conclusions of the testing program. The equipment qualification testing program was developed in accordance with EPRI TR-107330. The testing was performed at Wyle Laboratories in Huntsville, Alabama. Software qualification is discussed in Section 10.

9.2 System Qualification Test Plan

9.2.1 Scope

The technical scope, focus, and content of EPRI TR-107330 define the basis for the steps involved in completing a generic qualification program. Accomplishing the qualification requires creation of a Test synthetic application program (TSAP). The qualification steps are:

- A. The HFC-6000 product line was selected by HFC for qualification for nuclear safety applications.
- B. An evaluation of the HFC-6000 was performed. It was concluded that the HFC-6000 system, when fully and successfully tested in accordance with the EPRI TR-107330 and Regulatory Guide 1.180 Rev 01, was suitable to support nuclear safety-related applications.
- C. A set of hardware test modules with supporting software was defined and used as the HFC-6000 qualification Test Specimen. The specific set of hardware modules and supporting software are defined in the Section 1 Table 1-1.
- D. A Test System Application Program (TSAP) was defined and the software developed. The TSAP serves as a synthetic application that is designed to aid in the qualification and operability tests.
- E. The Test Specimen and the TSAP were combined into a test configuration and a set of acceptance tests was performed. This activity constitutes the system integration testing for the Test Specimen.
- F. A set of qualification tests to be performed on the Test Specimen was specified, including a defined set of Operability and Prudence tests to be conducted at suitable times in the qualification process.

G. The qualification tests were performed and the results documented. Documentation of results includes definition of the qualification envelope and identification of the specific products that were qualified.

This Section 9 addresses items A through G.

9.2.2 Equipment Tested

A qualification Test Specimen was designed to serve as a representative sample of the HFC-6000 system architecture. The Test Specimen was configured to be consistent with the requirements of EPRI TR-107330, Section 4. The HFC-6000 system incorporates a combination of architectural features from pre-existing HFC product lines, and the overall Test Specimen included sufficient functional capabilities to encompass a significant range of applications.

[

] System layout drawings, wiring and power distribution diagrams, and assembly diagrams defined specific details of the hardware design for the Test Specimen. Test plans and procedures provided detailed requirements and instructions for equipment mounting and interfaces to be used for equipment testing. Qualification Test Reports define the tests results and related analyses. A TSAP was developed as new application code using the guidance in BTP-14 and installed in the master controller of the Test Specimen. Detailed requirements for the individual modules in the Test Specimen and the TSAP were defined in a TSAP Requirements Specification. Detailed configuration information, such as module serial numbers and software versions, were recorded in the Master Configuration List (MCL), which is included as part of the qualification documentation.

9.2.3 Safety Functions Tested

The Test Specimen defined by HFC covered a subset of functional capabilities presented in EPRI TR-107330, Section 4. The specific capabilities demonstrated by the HFC qualification testing were as follows:

1. The capability of the Test Specimen to perform defined design functions within specified tolerances under normal environmental and operating conditions.
2. The capability of the Test Specimen to perform design functions within specified tolerances under the stressed conditions defined in EPRI TR-107330, Sections 5 and 6. Specific stress conditions demonstrated the capability of the Test Specimen 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
- Demonstrate specified levels of Class 1E isolation and continue functioning after application of the test voltage levels.

9.2.4 Test Requirements

The qualification Test Specimen was subjected both to a set of prequalification tests, a set of qualification tests, and a set of post qualification tests as illustrated in Figure 9.2. These tests served two primary purposes:

- Tests conducted prior to the start of qualification testing confirmed that the synthetic TSAP created for qualification testing purposes and the integrated hardware operated as intended.
- Operability and Prudency tests established a performance baseline for the Test Specimen. These tests were repeated at various points before, during and after the qualification test to demonstrate that the system performance remained within acceptable limits.

The qualification tests exposed the Test Specimen to a specifically defined set of abnormal conditions as defined in EPRI TR-107330. The purpose of these tests was to demonstrate the capability of the system hardware and software to continue operating within specified tolerances under extreme conditions.

9.2.4.1 Test Plans and Procedures

The following test plans and test procedures were prepared as part of the Equipment Qualification Program:

TN0401	Master Test Plan
TP0401	System Setup and Checkout Procedure
TP0408	TSAP Validation Test Procedure
TP0402	Operability Test Procedure
TP0403	Prudency Test Procedure
TP0404	Environmental Stress Test Procedure
TP0407	EMI/RFI Test Procedure
TP0409	ESD Test Procedure
TP0406	Surge Withstand Test Procedure
TP0405	Seismic Test Procedure
TP0410	Burn-in Test
TP0411	Isolation Test Procedure

The master test plan provides a link between the guidance of the EPRI TR-107330 standard and the procedures that were used to conduct the tests. The test plan addresses the general approach for the test program, and it included a separate test plan for each qualification test to be performed. Individual test plans for each test are included as attachments to the Master Test Plan, and each one identifies requirements, testing criteria, acceptance criteria, and documentation for a particular test.

The test procedures provided step-by-step instructions for conducting the tests and recording the results. These instructions included setup of equipment, test equipment requirements, environmental requirements, and procedural steps for conducting the tests, acceptance criteria, and tolerances.

[

]

Figure 9-1 - Test Data Flow Chart

9.2.4.2 Test Sequence

Figure 9.2 illustrates the overall sequence of the test program for this project. This figure shows the test program consists of separate prequalification and qualification test phases. The requirements, design, manufacture, and assembly phases of the life cycle were completed prior to the start of the qualification testing in accordance with HFC procedures. Actual testing of the Test Specimen commenced with system integration.

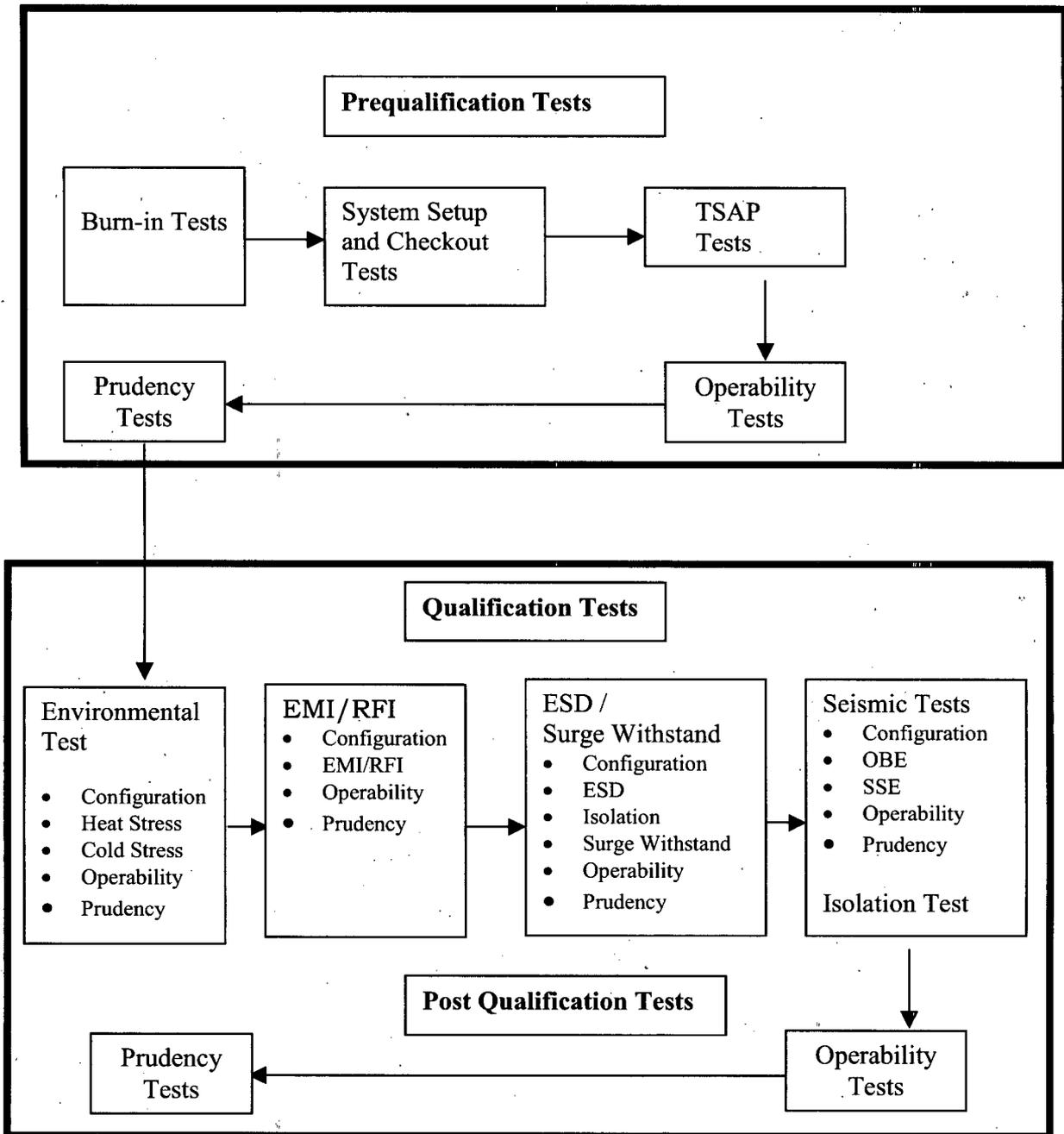


Figure 9-2 - Overall Test Sequence

NOTE

The EPRI standard required the environmental stress test to be performed first. No other specific sequence of execution was stipulated.

The prequalification phase was conducted by HFC test personnel at the HFC facility in Addison, Texas. The qualification tests were conducted at Wyle Laboratories. Wyle test personnel conducted the designated qualification tests based on requirements identified in the detailed test procedures. HFC test personnel were present to monitor and record performance of the Test Specimen. [

] Detailed requirements for each test were defined in the individual test plans included within the Master Test Plan. Detailed instructions for conducting the specific tests were contained in separate test procedures. Test results and the associated analyses are refined in the Qualification Reports.

9.2.4.3 Test Arrangement and Methodology

The test arrangement consisted of the Test Specimen connected to the HPAT controller and a PC workstation that are separate from the Test Specimen. The HPAT tester consisted of a separate HFC controller equipped with a test application program and a set of I/O modules configured to provide simulated inputs for the Test Specimen. The PC workstation was equipped with a standard set of HFC configuration, interactive graphics, and data logging software tools linked to both the HPAT and the Test Specimen. This arrangement permitted the test engineer to start/stop selected test routines and to record test results in the HAS and SOE data loggers.

During the prequalification testing phase, the Test Specimen was configured and subjected to a series of hardware, software, and functional tests. The TSAP was installed in the Test Specimen controllers, and its functional operation was verified. The TSAP included a set of simulated applications for safety system functions as well as algorithms specifically developed to support Operability and Prudency testing. The purposes for this phase of testing were as follows:

- Establish functionality of the software objects available to the TSAP.
- Verify functional operation of the TSAP.
- Validate operation of the automated test sequences.

- Establish an operational baseline for the Test Specimen.
- Document calibration and linearity of AI and AO modules included in the Test Specimen.

During the qualification tests, the Test Specimen was subjected to stress conditions to simulate various stress factors. While each test was in progress, the TSAP was processing test signal waveforms supplied by the HPAT. Responses of the Test Specimen during each qualification test were logged and compared to the performance baseline established during prequalification testing to detect any deviation in performance. After all of the qualification stress tests were completed, Operability and Prudency tests were repeated, and all responses were recorded and compared with the performance baseline to identify any degradation in performance. In each case, the logged responses of the Test Specimen provided the objective basis for evaluating the performance of the generic modular control system design.

9.2.4.4 Test Personnel

All prequalification test activities were conducted by one or more qualified HFC test engineers and test technicians. Qualification tests that required specialized test equipment (e.g., seismic, environmental, and EMI/RFI testing) were conducted for HFC by Wyle Laboratories personnel. HFC test personnel were present and conducted specified portions of the Operability and Prudency tests during these qualification tests.

9.2.4.5 System Operational Stress Conditions

EPRI TR-107330, Paragraph 6.3.1 identifies the major aging factors associated with a computer-based control system. The following sequence of tests exposed the qualification system to conditions that simulate the following stress factors:

- Environmental stress test. This test exposed the Test Specimen to abnormal combinations of high/low temperature and humidity.
- Pre-aging of relays and associated logic during prudency tests.
- Electrostatic Discharge test.
- Electromagnetic Interference/Radio Frequency Interference (EMI/RFI) test.
- Surge Withstand test.
- Seismic test.
- Isolation test. This test demonstrated Class 1E isolation of specified ports.

Each test exposed the Test Specimen to abnormal stress conditions while it was powered up and running the TSAP. The EPRI specification and Regulatory Guide provides detailed requirements for test parameters and the order in which particular tests are to be conducted. These requirements were incorporated into the individual test plans and illustrated in the test sequence diagram (Figure 9.2).

[

9.3 System Qualification Test Results

9.3.1 Prequalification Tests

The Prequalification Tests consisted of the Burn-In Test, System Setup and Checkout Test, TSAP Validation Test, Operability Tests, and Prudency Tests as shown in Figure 9.2.

9.3.1.1 Burn-in Test (TP0410)

The circuit card assemblies for the HFC-6000 Test Specimen were run in a normal operating environment for a minimum period of 352 hours prior to system integration in accordance with the Burn-in Test Procedure. The purpose of this test was to detect any early-life failures of component circuit cards. The scope of this test included two and a half times the total number of cards required for the complete Test Specimen. Circuit card assemblies not included in the initial test configuration of the Test Specimen were reserved as spares to be used as replacements for any cards that failed during the subsequent qualification tests.

The test engineers maintained a separate test record for each card being tested. The test record included the following information:

- Card name, part number, serial number, and software ID.
- Card rack and slot designation (if applicable) for burn-in test.
- Date and time burn-in test started.
- Date and time when burn-in test ended successfully.
- Date and time when card was removed from the burn-in test.
- Description of equipment failure (if any).

9.3.1.1.1 Burn-in Test Results

All assemblies to be utilized in the qualification test program passed the burn-in test by successfully achieving the minimum cumulative 352 hours of burn-in operation.

9.3.1.2 System Setup and Checkout (TP0401)

The System Setup and Checkout Tests were performed to verify that the project specified hardware, wiring and communication cabling had been installed and that communication had been established over each communication link, prior to the TSAP Validation Test.

Included in the Scope of this testing were the following activities/results:

[

]

9.3.1.2.1 System Setup and Checkout Test Results

All assemblies met the acceptance criteria for the setup and checkout tests.

9.3.1.3 TSAP Validation Test Procedure (TP0408)

The HFC-6000 system Test Specimen had a test synthetic application program (TSAP) installed that included sample control logic for power plant processes as well as logic to support automated qualification testing. The TSAP Validation Test Procedure validated the following activities:

[

]

9.3.1.3.1 TSAP Test Results

All TSAP software met the acceptance criteria.

9.3.2 Pre-Qualification Tests

9.3.2.1 Operability Tests (TP0402)

The following set of Operability tests was performed following completion of the TSAP tests described above. The purpose of these operability tests was to establish the performance baseline for the system. This performance baseline was then used as the basis for evaluating system performance during and/or following each of the qualification tests required by the EPRI standard.

- **Accuracy Test** - This test developed a baseline to compare against the accuracy and linearity of the analog I/O modules observed during the qualification tests.
- **Discrete Input Operability Test** - This test verified the capability of discrete input channels to detect a transition in the input signal being monitored.
- **Discrete Output Operability Test** - This test verified the capability of discrete output channels to operate reliably within its specified loading conditions.
- **Communication Operability Test** – This test verified reliable data transfer over the ICL and the C-Link
- **Timer Test** – This test developed the baseline for the timer function accessible to the TSAP.
- **Failover Operability Test** – This test demonstrated correct operation of the failover function.
- **Loss of Power Test** – This test demonstrated correct response of all I/O channels to a loss of source power followed by reapplication of power to the system.
- **Power Interruption Test** – This test demonstrated the capability of the power modules to sustain system operation during a temporary (40-ms transient) power interruption.
- **Power Quality Tolerance Test** – This test was developed to demonstrate the capability of the Test Specimen to continue normal operation over a range of source power voltages and frequencies. The Power Quality Tolerance Test was not part of the Operability Tests; it was required during the high temperature phase of the environmental test and after the completion of the seismic test only.

All tests, with the exception of the Power Quality Tolerance Test, were performed at the HFC site prior to shipment of the equipment to Wyle labs. The Power Quality Tolerance Test was performed at Wyle as specified in the HFC Operability Test Procedure.

9.3.2.1.1 Operability Test Results

The acceptance criteria defined for the operability tests were met with the exception of the following findings

SOE Test Data

During the initial baseline tests, some of the SOE test data for the Operability Test and Prudency Test was overwritten during the test period due to a fault in the test data recording process. The digital input (DI) modules that provided the SOE function contained a circular buffer for logging SOE data as it was received. Due to the circular nature of the buffer, when its storage capacity is exceeded, the earliest recorded data is overwritten. This problem was detected and corrected prior to the final Operability Test and Prudency Test. Subsequent Operability and Prudency test results were used to supplement the lost data and verify the acceptability of the SOE test results.

The objective of the initial baseline test was to establish baseline performance characteristics for comparison with performance before, during, and after subsequent Test Specimen stress tests. While the loss of part of this initial baseline SOE data occurred, it did not present a problem during execution and analyses of the subsequent qualification test results.

After the SOE data recorder was returned to the HFC facility, the problems with the SOE data storage were resolved and the Operability and Prudency Tests were performed again during post qualification testing. Complete SOE test data was obtained for these retests. 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.

Since the performance of the equipment after experiencing the environmental stress of the qualification program was acceptable, the performance of the equipment before the stress tests would also have been acceptable. The use of post stress test data to supplement pre stress test data was deemed to be acceptable.

HFC concluded that the loss of certain initial SOE test data for these tests, when supplemented by the additional test data from subsequent tests, had no adverse impact on the qualification test program.

Analog Input and RTD Input Modules Out of Calibration

The analog I/O modules have a specified design accuracy of 0.1% over their entire operating range. The Analog Input and RTD Input modules had individual channels whose performance was outside of this accuracy range during the initial performance of the Operability and Prudency tests. This was not detected prior to completion of the stress testing. Although out of calibration, the Analog Input and RTD Input modules tested during the subsequent stress tests operated consistently with the initial baseline test results. This allowed HFC to analyze the stress

test results and reach conclusions on acceptability. The stress conditions did not change the accuracy of these modules relative to the baseline accuracy for the modules.

After return of the Test Specimen to HFC, the post test was run with the cards as they were during the stress test. When the calibration problem was detected, a module was recalibrated to demonstrate that all channels could be restored to within the 0.1% accuracy range.

As defined in Section 9.2.4.2 item 17, the seismic test was preformed for the second time. When the decision was made to rerun the entire seismic test, all of the analog modules were recalibrated and retested before returning to Wyle. During this test, the calibrated analog I/O modules all performed within the specified 0.1% acceptance criteria.

HFC concluded that the out of calibration Analog Input and RTD Input cards had no impact on the performance of the qualification tests and had no impact on the ability to reach conclusions on the acceptance of the qualification test program.

9.3.2.1.2 Conclusion

HFC has concluded that these findings for the baseline Operability and Prudency tests had no adverse impact on the ability to evaluate the data and reach conclusions on the qualification test results.

9.3.2.2 Power Interruption Test

The HFC-6000 system operates with redundant 24 volt dc and redundant 48 volt dc power supplies. The power interruption test required a 40-ms interruption in the primary AC power line to the Test Specimen. When this disruption was imposed with all spare slots filled with operating modules, the internal power supplies for one or more of the modules went through the resetting cycle. After the AC power source was restored normal operation resumed.

Essentially all nuclear power plants have redundant sources of AC power for each safety channel. The HFC-6000 system was designed to operate with redundant AC power source connected to each safety channel to provide its redundant power to the redundant power supplies. Based on the single failure criterion, only one power source will experience a power interruption at any time, ensuring that the system will successfully maintain normal operation without resetting during that interruption.

9.3.2.2.1 Conclusion

HFC will define an interface requirement that all nuclear installations using HFC-6000 include two independent power sources with automatic switchover for each safety division to ensure that the system can sustain a 40-ms interruption in one power source without disruption to any control function.

9.3.2.3 Prudency Tests (TP0403)

The initial execution of the Prudency Tests was performed during the same time period as that of the Operability tests. These tests, as defined by the EPRI standard, do not address any specific requirement but exercise the Test Specimen in various ways to simulate potential stresses. Throughout the period that the Prudency tests were running the Test Specimen power source was set to 90 vac and 57 Hz to maximize operational stress. The following specific tests were defined:

- **Burst of Events Test** - This test was configured to impose a large number of operations on the HFC-6000 test specimen simultaneously in accordance with EPRI TR-107330, paragraph 5.4.A. This test was automated and was typically run as a continuous background operation for selected qualification tests.
- **Serial Port Failure Test** – The Test Specimen has two redundant serial communication links. For each link, this test imposed three simulated failures on a single channel of a redundant link; one failure condition at a time, transmit line open, transmit line shorted to ground, and transmit line shorted to receive line.
- **Serial Port Noise Test** - This test required introduction of a white noise signal on of the serial link one port at a time.
- **Fault Simulation Test** – This test required introduction of a simulated failure condition in the primary controller to trigger failover to the secondary controller. The intent of this test was covered by the Failover Operability test (TP0402) and so was not repeated as part of the Prudency tests.

The Prudency tests were executed during the prequalification phase of testing to establish a performance baseline for the Test Specimen. The BOE test was repeated at various points during the qualification stress tests to identify any performance degradation from the performance baseline, and the entire test was repeated following return of the equipment from Wyle Laboratory. The test data was captured and recorded by both the SOE and the HAS. The SOE system has a 1 ms response time for digital data only. The HAS can log both analog and digital data.

9.3.2.3.1 Prudency BOE Test Results

The acceptance criteria defined for the Prudency tests were met with the exception of minor deviations caused by problems with test setup or methodology. These include:

Loss of SOE Test Data

This matter was covered in the earlier Section on Operability Tests.

Automated Test Result Tolerance

This matter was covered in the earlier Section on Operability Tests

Conclusion

The deviations encountered were due to problems with test setup or methodology and not actual deviations in system performance. HFC has concluded that the deviations that occurred during the baseline testing had no adverse impact on the ability to evaluate those results and reach conclusions on the qualification test results.

9.3.2.3.2 Prudency Serial Port Failure Test Results

The Serial Port Failure test section of the Prudency test is configured to test the two redundant communication links in the Test Specimen. These are the (1) the C-Link between the controllers in the system, and (2) the ICL, which enables communication between the HFC-SBC06 and all input/output modules associated with a particular controller. The objective of the Serial Port Failure Test is to demonstrate that a hardware failure on a single serial link will have no adverse impact on the steady-state operation of the controller.

The Serial Port Failure test was run on the C-Link and the ICL during the prequalification phase of the program, and no transient disruption of the BOE waveform was detected at the moment the failure conditions were introduced or during subsequent steady-state operation. A full set of test data was available for the Post Qualification Testing and the only perturbation recorded was caused by the stopping the BOE test. The acceptance criteria were met.

Conclusion

No hardware failures (transmit line open, shorted to ground, or shorted to receive line) on a single serial communication channel produced either a transient or steady-state disruption in the performance of the controller.

9.3.2.3.3 Prudency Serial Port Noise Test Results

The Serial Port Noise test was designed to superimpose a white noise signal on either the transmit signal or the receive signal line of each serial link (one channel of the redundant pair) one at a time. This test was run after return of the equipment from Wyle.

The Serial Port Noise test procedure was written based on the use of a standard function signal generator. EPRI TR-107330 stipulates a 30 to 100 kHz white noise signal at 2.5 vrms. HFC substituted a 100 kHz saw tooth signal at 2.5 vrms with frequency modulation. This noise signal was used for testing the C-Link and the ICL.

The acceptance criterion for this test is that the BOE signal characteristics do not deviate by more than $\pm 10\%$ while the failure condition is being imposed.

Conclusion

The sweep modulated noise signal used for this test does not have the precise characteristics or frequency range of the white noise signal defined by the EPRI specification. HFC has concluded that the test using the substitute noise signal meets the intent of the original test requirements.

[

]

9.3.3 Qualification Tests

The Qualification Tests consisted of the following tests: Environmental, EMI/RFI/ESD, Surge Withstand, Seismic, and Isolation as shown in Figure 9.2. Portions of the Operability Tests and Prudency Tests were repeated several times throughout these test sequences, as indicated in the detailed test procedure covering each test and as specified in the EPRI TR.

9.3.3.1 Environmental Stress Test (TP0404)

The environmental stress test is one of the tests described by EPRI TR-107330 to qualify a commercially available PLC for safety-related applications in a nuclear power plant. This test exposes a specially configured HFC-6000 Test Specimen to extremes of temperature and humidity in order to induce accelerated aging of functional components. This testing was accomplished by enclosing the Test Specimen in an environmental test chamber in accordance with Wyle Laboratories Test Procedure 50043-1. The Test Specimen was running a 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 were conducted before, after, and at specified points during 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.

The environmental stress test consisted of three major phases (Figure 9.3):

- A minimum 48-hour period with the ambient temperature at $140^{\circ} \pm 5^{\circ}$ F and a relative humidity (RH) of $90\% \pm 5\%$ (non-condensing).
- A transition period of 4 hours during which the ambient temperature was reduced to $40^{\circ} \pm 5^{\circ}$ F with 0% to 10% RH (non-condensing).
- A minimum 8-hour period with the ambient temperature at $40^{\circ} \pm 5^{\circ}$ F with 0% to 10% RH (non-condensing).
- A transition period of 4 hours during which the test chamber was brought back to ambient room temperature and humidity.

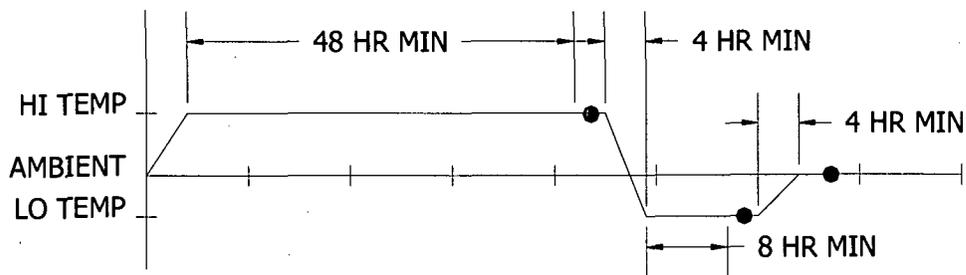


Figure 9-3 - Environmental Stress Temperature Profile

9.3.3.1.1 Environmental Test Results

The following evaluations and conclusions were reached regarding the environmental test results:

Power Drop to Test Specimen

[

]

HFC concluded that the intermittent shutdowns due to tripping of the power drop had no adverse impact on the test, nor did it affect the ability to reach conclusions on the test results.

[

] **RTD Module**
[

] **AI Module**
[

] **Conclusions**

The environmental test results show that the overall HFC6000 control system met all acceptance criteria [

1
9.3.3.2 EMI/RFI Test (TP0407)

The HFC-6000 Test Specimen is designed to operate in a wide variety of industrial applications. Both the HFC system hardware and the field equipment generate electromagnetic radiation (noise). The operation of the HFC system was tested to determine the susceptibility to EMI/RFI noise and the magnitude of EMI/RFI noise generated. This test sequence covered a series of four separate tests. During the first two tests, the Test Specimen was exposed to an external source of EMI/RFI, and the functional operation of the equipment was examined for signs of degraded operation. During the remaining two tests, the Test Specimen was configured for normal operation, and the magnitude of electromagnetic radiation generated by the equipment was measured.

The overall test requirements are defined by EPRI TR-107330-R1 and Regulatory Guide 1.180 Rev 1. The levels of EMI/RFI susceptibility and radiation limits are defined in Regulatory Guide 1.180 Rev 1. The test was conducted at Wyle Laboratories based on Wyle Test Procedure 50044-10. [

]

The susceptibility tests consisted of exposing the Test Specimen to a radiated or conducted electronic noise signal and monitoring functional operation of the control logic for abnormal operation. Wyle test personnel provided the EMI/RFI signal source and controlled injection of the test waveform to the Test Specimen. HFC test personnel controlled and monitored the functional operation of the Test Specimen. During each portion of the test, HFC test personnel ran specified portions of the Operability and Prudency tests and monitored operation of the Test Specimen for signs of susceptibility.

The radiated susceptibility test was divided into several frequency ranges with a different signal source and antenna for each frequency range. Each test 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 run at 30 Hz and 50 kHz. These test signals were injected directly into power leads of the Test Specimen. The test was executed for power module A of the redundant power supply (Model Jasper HML 601-5).

The high frequency conducted susceptibility tests were run between 50 kHz and 400 MHz. These test signals were inductively coupled into the power leads of the Test Specimen.

Wyle test personnel performed radiated magnetic and electric field emissions tests in accordance with Wyle Test Procedure 50044-10 Appendices D and E. EPRI TR-102323-R1 Chapter 7 was used to define power plant emissions limits and acceptable methods to be used for measuring these emissions levels. In addition, MIL-STD-461D RE101 was used to define the test method to be employed for measuring magnetic field emissions between 30 Hz and 100 kHz, and MIL-STD-461D RE102 was used to define methods for measuring radiated electric field emissions between 10 kHz and 1 GHz. Specified portions of the Operability and Prudency tests were run during the test to ensure that a minimum level of controller activity was present while the measurements were being run. [

]

Wyle test personnel executed conducted emissions tests in accordance with Wyle Test Procedure 50044-10 Appendices B and C. The tests were performed in accordance with EPRI TR-102323-R1 Chapter 7, which covers power plant emissions limits and acceptable methods to be used for measuring these emissions levels.]

9.3.3.2.1 EMI/RFI Tests Results

During the test, 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. In any power plant application, the HFC-6000 equipment will be installed in cabinets qualified for Class 1E applications. Such cabinets will provide shielding against external radiation, improving the overall radiation withstand capacity of the system. Furthermore, varied noise filters would be installed on certain power lines to lower emission levels at that source.

HFC has performed EMI/RFI tests for the Korea Ulchin 5&6 Nuclear Plant safety system project. The test specimen for this Korea system was composed of assemblies similar to the HFC-6000 Test Specimen,]

] The results for that test were satisfactory for all frequency ranges included in the test.

The results of each test are summarized below.

[

]

Low Frequency Radiated Emissions (RE101)

The HFC-6000 Control System was monitored in accordance with the RE101 Radiated Emissions Test procedure to measure the magnetic field emissions in the range from 30 HZ to 100 KHZ. All radiated emissions were within the specified limits over the entire frequency range.

High Frequency Radiated Emissions (RE102)

An evaluation was performed of the HFC-6000 radiated emissions from horizontal and vertical antennas positioned one meter from the front and one meter from the rear of the Test Specimen. The purpose of the test was to measure the electric field emissions from 10 KHZ to 1 GHZ relative to the criteria in EPRI TR-102323-R1. HFC later re-evaluated the emissions relative to the guidance in Regulatory Guide 1.180-Revision 1. The results below are based on this reevaluation:

[

] Substantially the same components have been qualified in such a cabinet during the development for the Ulchin nuclear power plant, and the HFC-6000 control system will be qualified in equivalent cabinet structures on a project by project basis. The Ulchin EMI/RFI test data is documented in the HFC documentation files.

Low Frequency Conducted Emissions (CE101)

The CE101 Conducted Emission Test was performed on the HFC6000 Test Specimen to measure emissions in the range of 30 Hz to 50 kHz range on all power leads. The conducted emissions on all power lines were within the specified limits.

High Frequency Conducted Emissions (CE102)

The CE-102 Conducted Emissions Test was performed on all power leads of the HFC-6000 Test Specimen to measure emissions in the range from 50 KHZ to 400 MHZ. Based on the acceptance criteria in USNRC Regulatory Guide 1.180 Rev 1, there are no anomalies in the frequency range covered by CS102.

Conclusions

[

]

9.3.3.3 ESD Test (TP0409)

Components of a HFC-6000 control system may be installed in an electrical equipment room as well as at various locations near the field equipment under control. In either case, the potential exists for exposure of sensitive electronic components to high voltage electrostatic discharges (ESD). This test subjects each component of the HFC-6000 Test Specimen to simulated ESD pulses to establish its capability to withstand such discharges without disabling or disrupting normal operation.

Detailed requirements for ESD immunity are defined by EPRI TR-102323-R1; the specific level of ESD immunity required is defined in EPRI TR-102323-R1 Appendix B Paragraph 3.5. ESD testing was conducted by Wyle Laboratories based on Wyle Test Procedure 50044-10 Appendix I. The test methods used to apply the ESD pulses are defined by IEC 61000-4-2 (equivalent to IEC 801-2).

Overall acceptance criteria specified by the EPRI specification are as follows:

- Subjecting the system to the specified level of ESD shall not disrupt operation or cause damage.
- For redundant platforms, performance is satisfactory if the platform performs as intended after being subjected to the specified level of ESD.

9.3.3.3.1 ESD Test Results

[

]

Conclusion ESD

The ESD test was successful.

9.3.3.4 Surge Withstand Test (TP0406)

Power, electrical I/O signal lines, and hardwired communication cables may be exposed to high amplitude transient signals in the locations where control system hardware may be installed. These locations include an electrical equipment room and various other locations near the equipment under control. The test covered by this document injected a large amplitude surge waveform at specified points of the Test Specimen. 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 in accordance with EPRI TR-107330.

9.3.3.4.1 Surge Withstand Test

General acceptance criteria are that the Test Specimen shall continue operating satisfactorily during and after application of the test input waveforms without disruption of backplane signals or other data that could disable the capability of generating a trip. Specific acceptance criteria for each component subjected to the surge waveform shall be as follows:

- Application of surge waveform shall not damage any module, component, or channel other than those specific modules or circuits subjected to the test waveform.
- Channels or modules other than the one under test shall continue to operate within normal accuracy limits for those modules during and after application of the test waveform.
- Failure of a single controller of the redundant pair will not be considered a failure condition if the backup controller assumes normal operation for the Test Specimen.

- Failure of the particular channel or circuit under test will not be considered a failure of the Test Specimen if the circuit (e.g., power module) is redundant, if the failure does not disrupt overall operation of the Test Specimen, or the failure does not propagate to other channels or circuits.

9.3.3.4.2 Surge Withstand Test Results

The Test Specimen met all acceptance criteria. Some components were damaged as the result of the test pulses, but those damages were limited to the specific components under test and the remainder of the system continued operating normally before, during, and after application of the test waveform. No failures propagated to other modules.

[

]

Conclusion Surge Withstand Test

The HFC-6000 Test Specimen satisfactorily met all of the acceptance criteria for surge testing.

9.3.3.5 Seismic Tests (TP0405)

Seismic testing exposed the HFC-6000 Test Specimen to a set of dynamic spectra designed to simulate an Operating Basis Earthquake (OBE) and a Safety Shutdown Earthquake (SSE). This test spectrum defined by EPRI TR-107330 is shown in Figure 9.4. 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. The overall scope of testing consisted of the following phases:

- Initial setup and pretest for equipment verification
- Low amplitude resonance search to identify critical frequencies below 100 Hz
- Five OBE
- One SSE
- Post seismic test inspection and operability test.

Various Operability and Prudence tests were run throughout the test sequence. Performance during these tests was monitored by a combination of:

- 24 accelerometers,
- The SOE logger with a total capacity of 48 digital points, and
- The HAS that has the capacity to log any point available from the operational data base of the controller

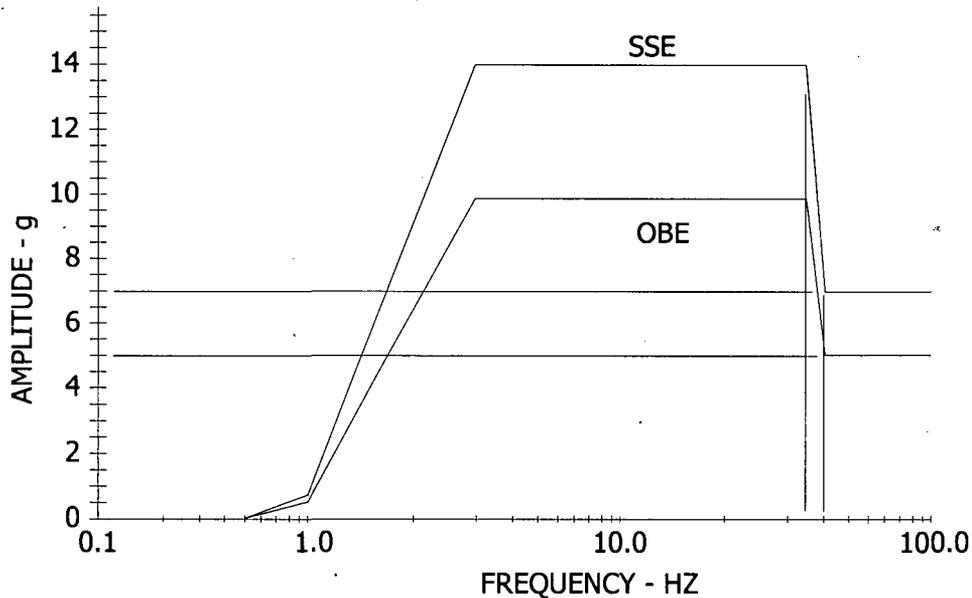


Figure 9-4 - Test Spectrum

A preliminary resonance test was conducted to determine if the Test Specimen components had any resonant frequencies within the RRS. The test was conducted by Wyle test personnel by imposing a low level sinusoidal sweep. If one or more resonant frequencies were detected, the Test Response Spectrum (TRS) was to be centered on the resonant frequency that produced the

maximum response in the Test Specimen. Overall requirements for the resonance search were governed by IEEE Std 344.

[

]

9.3.3.5.1 Seismic Test Sequence

The initial seismic test was run after completion of the surge withstand test. According to the HFC qualification master test plan, the seismic test was scheduled to be conducted right after environmental test. The Seismic test was performed after the Surge Withstand test due to a Wyle scheduling conflict. This change of sequence did not result in any violation of the required standards.

HFC decided to repeat the entire seismic test because the Test Specimen experienced several anomalies and a fault in the data recorder resulted in incomplete data. The data recorder fault is test equipment and not part of the Test Specimen.

[

]

Results of TSAP Validation Test (TP0408B)

[

]

All functional characteristics of the Test Specimen were found to be satisfactory.

Results of Operability Test (TP0402)

The Operability Test was repeated in its entirety after completion of the TSAP Validation Test. During execution of this test, every point configured for the HAS logger was verified, every manual test was run, and every automated test was run.

All analog points were verified to be within design tolerance. All automated tests were within the tolerance limits that had previously been identified. All functional tests were within the limits identified during the previous baseline test results.

Results of Prudency Tests (TP0403)

All of the Prudency tests were run at this time except for the Fault Tolerance test. The reconfigured Test Specimen successfully met all acceptance criteria.

Results of Seismic Test 2

The Test Specimen successfully withstood all seismic tests and continued to function normally. The overall system performance was within baseline tolerance limits with a limited number of minor anomalies. [

]

Conclusion

The Test Specimen was subjected to OBE and SSE test spectra up to the limit of the Wyle seismic simulator table (10 g maximum acceleration). [

]

9.3.3.6 Isolation Test

The scope of this Isolation Topical Report includes Class 1E isolation. Any module that meets Class 1E isolation requirements will also meet the less rigorous requirements for Non-Class 1E isolation.

The term “channel” and “channel to channel” in this section of the report means a “port” on an I/O module and “port to port” interactions on I/O modules. I/O modules will have multiple channels.

The HFC-6000 hardware may be installed both in an electrical equipment room and at various other locations near the equipment under control. When I/O chassis are physically located in a remote location with respect to the controller hardware, they will be connected to the controller by means of a dedicated Fiber Optic communication link. This link will provide the mechanism for ensuring physical and electrical isolation between the I/O modules and the controller.

Specific testing was performed to demonstrate two categories of Class 1E isolation:

- A fault on one channel of an I/O module will not effect the operation of other channels on the same module
- A fault on one channel of an I/O module will not effect the operation of other modules in the system

The tests addressed channel-to-channel isolation and channel to module isolation for each of the individual I/O module types. The primary purpose of these tests was to demonstrate immunity to faults on the inputs to the I/O modules. 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. The general approach to testing consisted of two phases:

- First, selected channels were subjected to the maximum Class 1E isolation test signals. If the component under test exhibited acceptable isolation from other components within the system, application of additional test signals at lower fault levels was deemed unnecessary.

- If the component under test did not exhibit acceptable isolation in response to the initial maximum Class 1E test signal, additional testing at lower fault levels was conducted to determine the maximum test signal that could be applied to that type of channel without affecting performance of other portions of the Test Specimen.

The minimum acceptable level of channel-to-channel isolation for normal operation differs for each card type.]

9.3.3.6.1 Isolation Test Results

Acceptance criteria for Class 1E isolation is defined in EPRI-TR-107330 (4.6.4), IEEE Std 603, IEEE Std 384 and RG 1.75.

The isolation test results for the HFC-6000 I/O modules demonstrate that;

- No I/O channel other than the channel under test is affected by the test signal.
- No module other than the module under test is affected by the test signal.

The following I/O modules and qualification levels for channel to channel and module to module isolation resulted from the tests.

Isolation Test Results

Module	Type	Channel Isolation	Module Isolation
AI16F	4-20 mA AI	250 vdc, 40 vac	250 vdc, 283 vac

AI18M	RTD Input AI	250 vdc, 283 vac	250 vdc, 600 vac
DC34	48-vdc DI	250 vdc, 600 vac	250 vdc, 600 vac
DC33	48-vdc DI	250 vdc, 283 vac	250 vdc, 283 vac
DI16I	48-vdc	250 vdc, 600 vac	250 vdc, 600 vac
AI4K	Pulse Input	250 vdc, 600 vac	250 vdc, 600 vac
AO8F	Analog Output	250 vdc, 600 vac	250 vdc, 600 vac
DC33	AC Discrete Output	250 vdc, 283 vac	250 vdc, 283 vac
DC34	DC Discrete Output	250 vdc, 283 vac	250 vdc, 283 vac
DO8J	Relay Output	250 vdc, 600 vac	250 vdc, 600 vac

Conclusions

All HFC-6000 I/O modules tested met the acceptance criteria for isolation.

9.3.4 Post-Qualification Tests

The Post-Qualification Tests consisted of re-running the System Setup and Checkout, Operability, and Prudency Tests at HFC following the return of the equipment from Wyle labs after completion of the first round of qualification tests. The purpose of the Post-Qualification Tests is to prove that the HFC-6000 control system continued to operate properly after being subjected to the complete set of qualification tests.

All Operability tests, with the exception of the Power Quality Tolerance Test, were performed at the HFC site. All Prudency tests, with the exception of Serial Link Noise Test and Fault Simulation Test, were performed at the HFC site.

[

]

9.3.4.1 Setup and Check-Out Test Results

All assemblies met the acceptance criteria for the set-up and check-out test.

9.3.4.1.1 Operability Test Results

The Test Specimen met defined acceptance criteria[

]

Analog I/O Modules Out of Calibration

This problem is discussed in subsection 9.3.2.1.1. All analog I/O channels were recalibrated and met the performance criteria prior to the seismic retest.

9.3.4.1.2 Prudency Test Results

The acceptance criteria defined for the Prudency tests were met[

]

Conclusions

HFC concludes that the Test Specimen continued to operate within acceptable criteria. The results of these tests replaced the data that had been lost during the prequalification test to provide the baseline for evaluation the qualification test results.

9.4 Conclusion

HFC has concluded that the HFC-6000 hardware as defined in the Test Specimen is suitable for use in nuclear safety-related applications. This hardware dedication is based upon the qualification test results and required functions of safety system.

10 Software Qualification

For more than 25 years HFC has provided safety critical digital control systems to industrial customers for critical applications where system quality, reliability and availability are key considerations. The digital software based platforms for these applications have a significant documented history of successful operation in these applications. HFC-6000 is the dedicated product line for safety related I&C platform applications for nuclear power plants. Software design and qualification are a critical aspect to the HFC dedication to high reliability and high availability systems. The basis for the qualification of safety related software for the HFC-6000 is taken from NUREG-0800, Chapter 7, Instrumentation and Controls. The HFC approach is also based on guidance provided in IEEE Std 7-4.3.2, BTP 7-14, EPRI TR-107330 and 106439. Compliance is demonstrated with 10 CFR Appendix B requirements with this approach.

The qualification process of HFC-6000 safety related software includes:

1. The dedication of Pre-Developed Software (PDS)
2. The development of any new controller software and I/O firmware
3. The development of application software

This report concentrates primarily on Type 1 software since all existing software in the scope of this report is PDS. However, the process for the development of any new software (Type 2 above) including application software (Type 3 above) is discussed later in this Section. The PDS encompasses all of the pre-developed Controller Software and the I/O firmware used by the HFC-6000. The PDS, including its documentation and development practices, were evaluated against regulatory criteria. The PDS operating history was evaluated and used as part of the COTS dedication process. This is discussed in more detail below.

Types 2 and 3 software or firmware has the same development process in accordance with the existing HFC quality procedures and work instructions. HFC accepts that the PDS may change in the future and that any changes made to PDS will need to follow current development requirements and guidance. The actual plant specific application software defined by future plant specified requirements and plant specific qualification will be performed at a later date. The process for development of Type 2 and Type 3 software is defined in this Section. The HFC process for this software is in accordance with the life cycle guidance presented in BTP 7-14, RG 1.152 which endorses IEEE Std 7-4.3.2 and Chapter 7 of the SRP.

The process for software design, testing and configuration management for all HFC-6000 safety related software, legacy and new safety related software, is defined in this Section.

10.1 The Dedication of Pre-Developed Software (PDS)

10.1.1 Software Commercial Grade Dedication Overview

The pre-developed software (PDS) implemented in the HFC-6000 digital platform is used in previous HFC product lines and is currently in operation at many sites both nuclear and non-nuclear. HFC-6000 controller software and PDS I/O firmware are based upon what HFC used in the ECS-1200 product lines (models -02, -03, -04 and -05). The ECS product line had its beginning in 1982 and was modernized and improved to its final stage in 1996. Each subsequent ECS software revision more closely replicates the HFC-6000 Software and Firmware. HFC has records for all of the changes and evaluations that have been performed to date. HFC maintains a library for this software/firmware including all revisions made to date.]

]

Figure 10-1 - Software Commercial Grade Dedication

The Sections below provide additional details on the PDS dedication process that creates the equivalent level of assurance required by NRC.

10.1.1.1 Verification of Software Documentation

The design evaluation reviewed the product's suitability for nuclear safety-grade applications, including the examination of failure modes, evaluation of the design process and review of the documentation. [

]

10.1.1.2 Documentation Evaluation

[

]

10.1.1.3 Software and Validation Testing Program

HFC determined that supplemental testing for the existing PDS needed to be performed to provide further evidence of product quality and suitability for dedication for safety-grade application. [

]

Please refer to section 10.1.3 for a detailed description.

10.1.1.4 Operating History Evaluation

The software components to be utilized in the HFC-6000 safety applications were identified and the related operating history was evaluated. The evaluation of the operating history demonstrated that the software has significant experience in critical application, including Korean nuclear power plants. The software has been reliable for a long period of time with very few defects, supporting the conclusion that the inherent quality makes the software suitable for dedication for use in nuclear safety applications. The defects are discussed in the Table of operating history. Furthermore, it was concluded that the operating conditions in Korean plants were either similar to or even identical to the operating conditions that will be seen in US nuclear plants. The HFC-6000 software is an evolutionary product and, as a result, there have been

varied changes over the 20 plus years of history to this PDS. Each of these changes has been evaluated and the determination made that they did not alter the functional requirements or the basic architecture of the OS. All changes were minimal with impacts determined to be negligible. The HFC development and change process is strictly controlled and its integration into hardware is thoroughly tested. This is discussed further in section 10.1.4. The defects noted above are also discussed in the Operating History Section 10.1.4

10.1.2 Verification of Software and Documentation

HFC-6000 PDS is a field-proven commercial grade software product. The software is defined as “software components” and is used by related “hardware components”. Table 1.1 of this report provides a listing of the HFC-6000 hardware within the scope of this report. The software components reside on the hardware modules within this list.

10.1.2.1 Software Requirements

The requirements of the PDS software modules were documented in the Requirement Specification for HFC-6000 modules during the software dedication process.]

10.1.2.2 Software Design Specification

The HFC-6000 documentation scheme has a four layer arrangement; they are 1) Top Level, 2) Module Level, 3) Module Detail Level, and 4) Component Level. All dedicated software components require a complete design specification to illustrate the detail design of the software. The hardware specific software is defined in the higher level hardware module or module detail design specification. Software design specifications are provided in the HFC-6000 Product Line Documents set.

10.1.2.3 Software Dedication Process

[

]

10.1.2.4 Source Code Inspection

To support the software dedication process, HFC performed a complete source code inspection of the PDS. The goal of this inspection was to detect specific types of faults, violations with coding standards, and to verify the correctness of the code. This effort was a complement to the dynamic testing that was performed later. This code inspection effort is performed to complement the initial software design process and provides a different reviewer's perspective who can detect fault information overlooked by initial software design; and not detected in the initial dynamic testing. The code inspection is also used to develop additional test cases for future dynamic testing.]

]

In summary, the code inspection examined the program designs and its interactions to determine consistency with the functional requirements. This analysis also targeted the design structure, logic and the data structures. The translation of the design into software code and standard compliance were part of the static analysis. Discrepancies were identified and corrections were made to the source code. The detailed code inspection process and the results are discussed in the HFC Code Inspection Report.

10.1.3 Software Validation and Testing Program

Software Testing was performed in the following series of tests.

10.1.3.1 Application Software Object Tests

In this section the term “application software” means operating software objects associated with the systems level functions of the controller. Plant specific application code is not included in this report and review.

A comprehensive Application Object Test (AOT) was conducted on the HFC-6000 product line. This included all software components that have a direct impact on the application code or that can be accessed by application code while it is running on the system processor of the HFC-SBC06 controller module. Such software components are designated as Application Software Objects (ASO). The scope of this testing included both normal operations and exceptional conditions for the following ASOs:

[

]

During compilation of the application object, the offline compiler generates error reports if any errors occur. Any compiling errors will be identified before the object code to be executed in the controller is generated. Only the successful compiled application object is used to test with the controller module.

All tests required by the test procedure have been completed and all acceptance criteria have been met. The ASO test reports were reviewed and documented with no error reports.

10.1.3.2 Software Component Tests

A software component can be a software routine, function, task, operating system or sets of software files. All identified software components are PDS software that are classified as such and placed into the HFC software library. These software components are used in various hardware modules across the HFC product lines.

Software component tests were conducted on the software components that are used in the HFC-6000 product line. 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. A test design is based on the software functions described in the PDS documentation or the HFC-6000 product requirement specification. Test inputs were defined during design of the test cases and the expected outputs were determined. Since most of the software components are part of the printed circuit board firmware, software component testing is mostly low level code testing using an emulator to create a simulation testing environment. Test software including one or more software components were run on a representative hardware platform.

[

]

All major software components were tested and test reports were reviewed and documented. No critical defects were detected during these tests.

10.1.3.3 Functional Tests

The purpose of functional testing is to test the functionality of hardware modules and associated software components. The function test procedures and acceptance criteria were based on the requirement specifications. Functional testing was performed with the final release version of software. Any calibration sequences needed were included in the functional testing as a pre-set up.

All HFC-6000 hardware modules have gone through functional tests after production.[

]

All functional tests for the qualification software were completed and all acceptance criteria have been met. Test reports were reviewed and documented.

10.1.4 HFC-6000 Operating History

10.1.4.1 Operating History Background and Evaluation Approach

The HFC systems and the associated hardware and software have extensive operating history. HFC has concluded that high reliability hardware components and software modules are demonstrated in the historic operation of the HFC systems in the installed base.

[

]

The operating history evaluation is directed primarily at the controller software and I/O firmware. Critical defects are also evaluated for the software design.

The Operating History evaluation process included:

- Calculate the total hours of operation per software component type
- Define the critical software defects that occurred during the stated time period
- Calculate the critical software defects per hour of operation
- Evaluate the critical defects to show whether or not they would have an impact on the safety functions of the software module

10.1.4.2 HFC Product Lines

HFC has three product lines which are applicable to the operating history evaluation. They are:

AFS-1000	Boiler Safety and Nuclear Safety I &C system
ECS-1200	Plant Control System
HFC-6000	Nuclear Safety I &C system

The HFC-6000 product line incorporates many of the hardware and software features of the AFS-1000 and ECS-1200 product lines.]

10.1.4.3 Product line History

The AFS-1000 architecture is employed primarily for applications that employ single loop control of field equipment with its local I/O modules library. The product has been used for boiler safety applications. The ECS-1200 architecture is employed primarily for multi-loop Plant Control System (PCS) applications. The I/O modules can be connected either locally or remotely through RS-485 serial communication. Both product lines have extensive operating histories.

10.1.4.3.1 AFS-1000 Product line History

The following table illustrates the HFC AFS-1000 product line history.

Table 10-1 – AFS-1000 Product line history

]

10.1.4.3.2 ECS-1200 Product line History

The following table illustrates the HFC ECS-1200 product line history.

Table 10-2 – ECS-1200 Product line history

]

]

10.1.4.4 Relationship of HFC-6000 product line to the AFS-1000 product line

Table 10-1 shows the relationship of the HFC-6000 to the AFS-1000 product line. The software of the two product lines is essentially the same design with the exceptions of different coding for the earlier versions of the microprocessors. However, the HFC-6000 inherited not only the special I/O circuitry for nuclear safety I & C system but also the control system logics were merged into HFC control algorithms as the base of critical mission control algorithms.]

]Any changes made to HFC-6000 software will be made under the new process conforming to full safety quality requirements.

10.1.4.5 Relationship of HFC-6000 product line to the ECS-1200 product line

Table 10-2 shows that the HFC-6000 hardware and software are essentially identical to the existing ECS-1200 product line with the exception of changes in the form factor.[

] Table 10-2 also shows that the basic system software modules used in the HFC-6000 are the subset of basic system software modules that have been used in the ECS-1200. This includes the operating system, controller, communications and I/O software.

10.1.4.6 ECS-1200 Operating History

As discussed above, the HFC-6000 is a technology extension of the ECS-1200 using the same basic hardware components with form factor changes and with no changes in the basic system software modules.[

] *Table 10-3 - Key ECS-1200 Installations*

[

Table 10-4 - TMOY Calculation

]

10.1.4.8 Determination on Critical/Non-critical Software Defects

Critical software defects are defined as “defects in the basic system software that prevent the associated hardware module from processing inputs and obtaining correct actuation outputs.”

[

]

Table 10-5 - Operating history and defect hours

]

10.1.4.9 Conclusions of defect analysis

[

] As a result, the summary of operating history for HFC-6000 application shows that, there have been no relevant critical software defects on any operating site for the ECS-1200 system since 1995.

10.1.4.10 Summary of Operating History

The evaluation of the operating history for HFC-6000 software components are based upon the real plant operating hours of existing ECS-1200 and applicable AFS-1000 control systems.

- AFS-1000 pre AFS-SBC-05 control systems (before 1995)

The excellent operating history of AFS-1000 systems provides the qualitative proof of the HFC design and application engineering process. [

-]]
- AFS-1000 SBC-05 control systems

The AFS-1000 SBC-05 had been used as the upgrade path for older AFS-1000 product line. [

-]]
- ECS-1200 Control System

The HFC-6000 software components are a subset of the ECS-1200 product line software. The operating history of the ECS-1200 control system has been used in the calculation of the TMOY. Based upon the above evaluation process and calculation, it proves the excellent reliability of these software components (The defect per hour data is from 2.44 E-08 to 3.9 E-08 and all were non-critical defects).

10.1.5 Software Operation and Maintenance

The HFC Software Operation and Maintenance program is applicable for both PDS and the application software for the HFC-6000 control system.

Figure 10-2 illustrates the quality control process of the HFC-6000 software.

[

]

Figure 10-2 - Software Operation and Maintenance

The operation and maintenance of HFC-6000 software is regulated by HF Controls Software Configuration Management (SCM) procedures and work instructions. The SCM identifies and dedicates the software components for the HF Controls product line. The identified SCM software components include source codes and executable codes.]

]The HFC SCM phases follow the applicable guidance in RG 1.169, IEEE Std 829 and IEEE Std 1042. The HFC SCM is applied to both PDS and new software.

10.1.5.1 Error Detection

HF Controls Corrective Action Program provides the governing procedure for HFC-6000 software error resolution tracking. Once the HF Controls software had been released, a Conditional Report (CR) is required when problems, non-conformances or conditions adverse to quality are discovered. This error detection and corrective process are implemented at the HF Control facility during factory testing and continuously at customer sites.

The Condition Review Group (CRG) is a management group consisting of as a minimum, Project Managers, QA Manager, Director of Operations and applicable Engineering Managers. This group meets on a regular basis. They are responsible for determining the category of Condition Reports, assignment of an appropriate manager responsible for the correction, and establishing the estimated completion date.

The responsible manager responds to the assigned CR with a problem investigation, and solution evaluation. The process of the error detection, dispositions and corrective actions are tracked by the Corrective Action Program. For critical errors, such as a software malfunction, impact to the

operation of customers, in addition to error solution tracking and a root cause analysis is required to prevent the similar issue happen in the future.

10.1.5.2 Error Correction Change Control

The change control process of software is managed through the HFC SCM procedures and the Change Control Tracker tools. This mechanism assures that the change process of the software component is accurately tracked at any given time. This change control software process provides the capability for using the HF Controls corporate network to “submit” change requests to the Software Management Team (SMT) and to record impacted component, implementation approval and implementation sign off process. It also provides connections between the change process and Version Manager utility software for component version control.

10.1.5.2.1 Change Management Levels of Authority

The manager of Development Engineering is the Category Owner (CO) and has the responsibility to handle the SCM activities of HFC-6000 software components regarding change request and impact analysis.

Once a change has been approved, the CO assigns one or more technically qualified individuals to implement the change. The implementation of the Software Change Request (SCR) shall be reviewed and approved by the CO and members of the Software Management Team (SMT). The members of the SMT include the senior management of engineering, the manager of QA and the V & V team leader.

10.1.5.2.2 Software Change Request (SCR)

The following table illustrates the complete cycle of the software change process.

Table 10-6 - Software Change Process

Step	Responsible Person	Actions
1	SCR Originator	1. Open, Edit & Submit SCR with ID 2. Notify Category Owner
2	Category Owner	1. Complete the impact analysis 2. Notify the Software Management Team for implementation approval
3	Software Management Team	1. Approve the change request 2. Notify Category Owner
4	Category Owner	1. Assign implementation engineer 2. Change Implementation Process, validation and review 3. Notify for implementation sign off
5	Software Management	1. Signoff implemented change

	Team	2. Notify Category Owner
6	Category Owner	1. Sign off SCR 2. Submit documents

10.1.5.2.3 Audits and Reviews

Both internal and external audits of the SCM process are performed. The QA Representative and V&V team perform the Internal Audits.

[

]

Reviews shall be conducted throughout the project life cycle phases. Various reviews are defined in the HF Controls ISO Design Review procedure.

10.1.5.3 Training

The HFC Department of Customer Care is the organization that oversees training including schedules and resources. The training facility includes the HFC-6000 safety platform qualification test bed and simulation equipment. HFC performs training courses includes system hardware, software, application programming, tools and system maintenance and trouble shooting. The simulation equipment with pre-fabricated programs can be used as either close loop or open loop tests. The service engineers of the Customer Care Department can also perform on-site training courses. A Software Training manual has been written that discusses HFC training processes.

10.1.5.4 Customer Reporting

HFC has QA procedures in place to provide HFC personnel with instructions relative to documenting, evaluating and reporting problems associated with the design, fabrication, assembly, testing and installation of nuclear related plant equipment in compliance with the reporting requirements of the Nuclear Regulatory Commission (NRC) Code of Federal Regulations (CFR) Title 10, Part 21, "Reporting of Defects and Noncompliance."

10.1.5.5 QA & CR Process

The HFC Quality Assurance Program Manual (QAPM) describes the Quality Assurance Program at HFC. The program is designed to provide administrative measures and procedures necessary for assuring that all HFC hardware and software products as well as any services meet or exceed customer requirements and applicable industry codes and standards. This Quality Program is designed to comply with ANSI/ASME NQA-1&1a-1994; *Quality Assurance Requirements for Nuclear Facilities*, (Basic Requirements) ANSI/ASME NQA-1a-1995

Addenda, 10 CFR 50 Appendix B; "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants", ISO 9001:2000, and 10CFR Part 21.

HFC's specific goals and objectives are to provide to our customers: 1) Quality products with no defects or failures, 2) Products delivered on or prior to the promised date 3) Continuous improvement of products and processes and 4) Services that exceed customer expectations. HFC also commits to continually broaden the knowledge base of our employees and services within a safe work environment.

The requirements of this manual apply to all activities affecting the quality of products and services provided and performed by HFC. HFC personnel at every level of the organization are required to fully support the HFC QA Program, achieve a high level of excellence through the application of proven technology in their respective areas of responsibility, and promote an atmosphere of continuous improvement.

Contractual arrangements between the customer and HFC, which specify requirements in addition to those specified by this Quality Program, are applied at the project level providing such requirements do not compromise the quality of our service or this Quality Program.

All non-conformance issues are handled through the Condition Report (CR) system as the control and tracking tool. The implementation of software changes as the solution for CR is handled in accordance with HFC software configuration management procedure and work instructions.

10.2 Safety Related Software Development

Any new software development process for the HFC-6000 is in accordance with the current HFC quality procedures and work instructions and follows the life-cycle guidance contained in BTP 7-14. All new software including the application software is controlled by this process once it is designated as safety related.

10.2.1 Software Development Life Cycle

Newly developed software will require V&V during each phase of development. Criteria for qualification of critical components are governed by the following standards:

- IEEE Std 1012-1998 provides the documentation requirements for V&V of both critical and non-critical components of software systems.
- IEEE Std 7-4.3.2-2003 provides additional guidance and standards for qualifying digital computer systems for use in safety systems of nuclear power plants.
- IEEE Std 603-1991 provides requirements for general qualification standards for digital systems to be used as part of a nuclear safety system.

- Regulatory Guide 1.168 augments guidance of IEEE Std 1012 for V&V of digital computer software used in safety systems of nuclear power systems.
- BTP 7-14 Provide Software Life Cycle guidance

RG 1.173 and IEEE Std 1074 provide a structured approach for the development of the HFC-6000 software life cycle program. HFC requires an orderly structure to the entire software design and implementation life cycle process. HFC's software life cycle addresses the issues and concerns of the requisite standards. The Software Life Cycle process that HFC uses provides the necessary framework for the HFC-6000 software project so that activities can be mapped. With this mapping, a concurrent execution of related activities can occur and staged checkpoints are available at which characteristics of certain activities can be verified.

[

]
Table 10-7 - Life-Cycle Phase Cross-Reference Chart

1
HFC's software test methods and procedures, tests conform to the guidance contained in RG 1.171. The software tests are performed and the results are required to meet test objectives within the pre-established criteria for the new software. HFC's software unit test methods and procedures, tests conform to the guidance contained in RG 1.172. The unit tests are performed and the results should meet all test objectives within the pre-established criteria for new software.

10.2.2 Life-Cycle Verification and Validation

This section defines the processes for new software/firmware development which includes all application software and any new modifications to the controller software and I/O firmware in accordance with BTP 7-14, IEEE Std 7-4.3.2 and IEEE Std 1012. The SVVP provides a detailed plan for each of the HFC-6000 system life-cycle phases. The following major topics apply to each phase of the life cycle.

- **V&V Tasks.** The V&V tasks constitute the activities of the V&V function throughout the software development life cycle. Depending on the particular life-cycle phase, these tasks may consist of generating plans, test procedures, and test cases or of using the previously generated plans and tests to evaluate particular new software components. The definition of V & V tasks are based on the tasks defined by IEEE Std 1012-1998 and Regulatory Guide 1.168 for safety system software.
- **Methods and Criteria.** These topics relate to the means by which particular software components are evaluated and the basis for pass/fail judgments. [

- **Inputs/Outputs.** [

The HFC V&V activities continue throughout the duration of product development project and nuclear system application project. For product development projects, V&V activities essentially end when the product is released for production. The HFC Software V&V Plan defines all V & V activities to be conducted for both a product development project and an application project.

10.2.2.1 Project Planning Phase

The primary guiding document for product development projects is the Product Development Plan (WI-ENG-11). A Project Quality Plan (QPP 2.1) provides the corresponding function for application projects. However, both product development and application projects begin with the existing HFC product lines as the starting design basis. [

]

10.2.2.2 Requirement Phase

The requirements phase of the project life cycle is the period during which specific functional, performance, and other requirements are identified and allocated to specific components. Detailed coverage for activities during this phase is provided by the following:

- QPP 5.2, "Preparation of Procedures"
- WI-ENG-002, "Design Inputs"
- WI-ENG-100, "Engineering Processes"
- WI-ENG-104, "Development of Hardware Requirements Specifications"
- WI-ENG-202, "Development of Software/Firmware Requirements Specifications"

In addition to the above work instructions that apply to all projects, a nuclear safety-related project may also require development of an Abnormal Conditions and Effects (ACE) list and requirements for remediation. This activity will be accomplished in accordance with specific contract requirements for such projects.

Task Inputs	Task Outputs
<ul style="list-style-type: none"> • Project Development Plan or Project Quality Plan • HFC V&V Program • Customer Specification • HFC Work Instructions • Qualification requirements defined by regulatory or industry standards 	Requirements Specifications Document Reviews Traceability Analysis ACE List

10.2.2.3 Design Phase

During the design phase, component requirements are converted into the detailed design for individual components, for a product line, or for a specific control system composed of standard components. [

] There are separate procedures for product development and application development.

10.2.2.3.1 *Product Development Project*

During this phase of a product development project, the defined design inputs are used to create a new design for a new standard HFC hardware or software product. All product development projects will be accomplished in accordance with Appendix B and NQA1 requirements. Detailed guidance for activities during this phase is provided by the following:

- QPP 5.2, “Preparation of Procedures”
- WI-ENG-001, “Design Verification and Reviews”
- WI-ENG-106, “Development of Hardware Design Specifications”
- WI-ENG-203, “Development of Software/Firmware Design Specification”

In addition to the above work instructions that apply to all product development projects, initial planning for product qualification begins at this stage of the lifecycle. Traceability analysis and evaluation of ACE immunity is undertaken as part of the review process for the completed design.

Task Inputs	Task Outputs
<ul style="list-style-type: none"> • Project Development Plan • Requirements Specification • Customer Specification • HFC Work Instructions • ACE List 	Requirements Specifications Hardware Schematic Diagrams Traceability Analysis Design Review FMEA (if required) Qualification Test Plan (if required) Qualification Test Procedures (if required)

10.2.2.3.2 Application Development Project

During this phase of an application development project, plant specific functional requirements are used to develop the application software.]

Task Inputs	Task Outputs
<ul style="list-style-type: none"> • Project Quality Plan • Requirements Specification • Customer Specification • HFC Work Instructions • ACE List (if required) 	Design Arrangement Drawings Schematic Diagrams Component Design and Assembly Drawings Logic Diagrams User Interface Design Traceability Analysis Design Review FMEA (if required)

10.2.2.4 Implementation Phase

The implementation phase of the life cycle is that period during which hardware components are fabricated and software code is developed. As before, different sequences are followed for product development and application projects.

10.2.2.4.1 *Product Development Project*

[

Task Inputs	Task Outputs
<ul style="list-style-type: none">• Project Development Plan• Design Specification• HFC Work Instructions• Engineering Drawings• Prototype Validation Test• ACE List (if required)	<ul style="list-style-type: none">Traceability AnalysisDesign ReviewPrototype Test ReportCR for nonconformanceQualification Test Report(s)FMEA Report (if required)

10.2.2.4.2 *Application Project*

Implementation for an application project consists of building the hardware designs and coding the software/firmware for that design. [

]

10.2.2.5 Integration and Testing Phase

This is the phase of an application project during which a complete control system is integrated together and tested as a unit. QC inspection of shop floor activities continues throughout this period, and generic integration/acceptance testing verifies system functional characteristics. [

]

Task Inputs	Task Outputs
<ul style="list-style-type: none"> • Project Quality Plan • HFC Work Instructions • Engineering Drawings • Process Control Sheets • System Acceptance Test Procedure • Test Procedures 	Traceability Analysis Test Reports CR for nonconformance

10.2.2.6 Deployment

After completion of acceptance testing, the product (individual hardware or software components or a completely integrated control system) is shipped for onsite installation. [

]

Task Inputs	Task Outputs
<ul style="list-style-type: none"> • Project Quality Plan • Customer PO • Engineering Drawings • Project-Specific Test Procedure 	System and Component Documentation Installation Test Report (if required)

10.2.2.7 Operation and Maintenance

Following delivery and onsite acceptance of a control system, the customer normally assumes responsibility for operation and the regular preventive maintenance of the system. HFC does provide field service and spare part support for all customers. HFC also supports 10 CFR Part 21 reporting and record keeping for nuclear projects. These activities are performed in accordance with;

- QPP 16.3, “10 CFR Part 21 Reporting”
- QPP 20.1, “Servicing and Customer-Supplied Products”
- WI-CUST-001, “After Market Service Activities”
- WI-CUST-002, “Return Material Authorization”

10.2.3 V&V REPORTING

V&V activities are conducted using the guidance provided in IEEE Std 1012 and RG 1.168 for the lifecycle phases for both product development and application projects. As each task is accomplished, the individual responsible for executing that task is responsible for producing a

written report that identifies what was done and describes any discrepancies that may have been detected. These reports constitute the objective evidence that the V&V task was completed and provide the mechanism for initiating remedial activities, if necessary.

10.2.3.1 V&V Task Report

V&V tasks include phased reviews of documents, tests, and analyses covering the software process. Each review and each formal test includes a report form that provides a mechanism for recording results and any observed discrepancies. Both review documents and test result forms are designated as Quality records and will be retained by Document Control. V&V task reports that are developed are supplied to the V&V Team Leader and will provide the basis for generating the System V&V Report. HFC policy is that the V&V Team Leader responsibility is independent of the design and development responsibility. The person assigned to a specific V&V activity shall not have been involved in the associated design activity.

10.2.3.2 V&V Analysis Report

A separate report is generated to cover each phase conducted during the course of the software process. [

]

Any abnormal conditions or findings that are adverse to quality or safety are reported in a Condition Report (CR).

10.2.3.3 Software V&V Report

The Software V&V Report (SVVR) is a formal summary document that describes V&V activities conducted throughout a particular project. When a project requires formal submittal of V&V reports, the content of the individual V&V task reports will be summarized on a phase-by-phase basis and supplied to the customer and maintained in the HFC library. This report is intended to provide objective evidence of the oversight and review/approval activities conducted throughout the project.

10.2.3.4 Condition Reports

A separate Condition Report (CR) shall be created for each distinct discrepancy or for a group of related discrepancies between observed task results and expected results. As a minimum, the person having primary responsibility for performing a particular task shall report all

discrepancies detected while performing that task. Other HFC personnel or customer personnel may report perceived deficiencies apart from any specific test, test procedure or test case. Any discrepancy (practice, condition, or malfunction) detrimental to quality shall be reported on a CR in accordance with HFC procedure QPP 16.1, "Corrective Action Program." All CRs shall be reviewed and tracked in accordance with QPP 16.1.

10.2.3.5 Final V&V Report

When a project requires formal V&V reporting as a deliverable item, the final V&V Report shall constitute the final submittal of the SVVR.]

]

HFC6000 Topical Report Review (MC5380)

[

1

REQUEST FOR ADDITIONAL INFORMATION (PART 2)
REVIEW OF HF CONTROLS CORPORATION REPORT
PP-901-000-01
"HFC-6000 SAFETY SYSTEM TOPICAL REPORT"
REVISION A
(NRC TAC MC5380)

I

Block	Description

Block	Description

AFFIDAVIT

STATE OF TEXAS

2008031907

COUNTY OF DALLAS

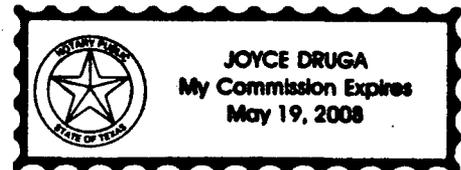
Before me, the undersigned authority, personally appeared Allen Hsu, who, being by me duly sworn according to law, deposes and says that he is authorized to execute this Affidavit on behalf of Doosan-HF Controls Corporation (HFC) and the averments of fact set forth in this Affidavit are true and correct to the best of his knowledge, information and belief:



Sworn to and subscribed
Before me this 19 day
Of March, 2008



Notary Public



- (1) I am Allen Hsu, President of the Doosan HF Controls (HFC) Corporation and as such, I have been specifically delegated the function of reviewing the proprietary information sought to be withheld from public disclosure in connection with nuclear power plant licensing and rulemaking proceedings, and am authorized to apply for its withholding on behalf of Doosan-HFC Corporation.
- (2) I am making this Affidavit in conformance with the provisions of 10 CFR Section 2.390 of the Commission's regulations and in conjunction with the Doosan HFC application for withholding accompanying this affidavit.
- (3) I have personal knowledge of the criteria and procedures utilized by Doosan HFC in designating information as trade secret, privileged or as confidential commercial or financial information.
- (4) Pursuant to the provisions of paragraph (b)(4) of Section 2.390 of the Commission's regulations, the following is furnished for consideration by the Commission in determining whether the information sought to be withheld from public disclosure should be withheld.
 - (a) The information sought to be withheld from public disclosure is owned and has been held in confidence by Doosan HFC Corporation.
 - (b) The information is of a type customarily held in confidence by Doosan HFC and not customarily disclosed to the public. Doosan HFC has a rational basis for determining the types of information customarily held in confidence by it and, in that connection, uses a uniform method to determine when and whether to hold certain types of information in confidence. The application of our method and the substance of constitute Doosan HFC's policy and provide the rational basis required.

Under the Doosan HFC method, information is held in confidence if it falls in one or more of several types of information, the release of which might result in the loss of an existing or potential competitive advantage as follows:

- ❖ Its use by a competitor would reduce his expenditure of resources and improve his competitive position in the design, manufacture, installation, assurance of quality, or licensing a digital based I&C system.
- ❖ It reveals cost or price information, production capacities, budget levels, or commercial strategies of Doosan HFC, its customers or suppliers.

- ❖ It reveals aspects of past, present or future Doosan HFC or customer funded development plans and programs of potential commercial value to Doosan HFC.
- ❖ It contains patentable ideas, for which patent protection may be desirable.

For this affidavit, all of the information marked proprietary is because its use by a competitor would reduce his expenditure of resources and improve his competitive position in the design, manufacture, installation, assurance of quality, or licensing a digital based I&C system (type one above). This leads to a Doosan HFC need to restrict certain commercial information from the public to prevent its use by competitors and creating a commercial advantage for them to the detriment of Doosan HFC.

The development of the HFC-6000 system design is the result of many years of development by uniquely experienced personnel in an intensive effort along with the expenditure of a considerable sum of money. In order for competitors to duplicate the Doosan HFC design and applicable information, similar technical programs would have to be performed and a significant manpower effort, having the requisite talent and experience would have to be expended for the development of a digital design to equal the HFC-6000 system design.

There are sound Doosan HFC policy reasons behind the Doosan HFC proprietary designation system which include the following:

- a) The Use of such information by Doosan HFC gives Doosan HFC a competitive advantage over its competitors. It is therefore, withheld from disclosure to protect the Doosan HFC competitive position.
- b) It is information which is marketable in many ways. The extent to which such information is available to competitors diminishes the Doosan HFC ability to sell products involving the use of the information.
- c) Use by our competitors would put Doosan HFC at a competitive disadvantage by reducing their expenditure or resources at Doosan HFC expense.
- d) Each component of proprietary information pertinent to a particular competitive advantage is potentially as valuable as the total competitive advantage. If competitors acquire components of proprietary information, any one component may be the key to the entire puzzle, thereby depriving Doosan HFC of a competitive advantage.

- e) Unrestricted disclosure would jeopardize the position of Doosan HFC in the world market such as South Korea, and thereby give a market advantage to the competition in those countries.
- (5) The information is being transmitted to the Commission in confidence and, under the provisions of 10 CFR 2.390, it is to be received in confidence by the Commission.
- (6) Available information has not been previously employed in the same original. The information sought to be protected is not available in public sources or manner or method to the best of our knowledge and belief.
- (7) The proprietary information sought to be withheld in the submittal is that which is appropriately marked by brackets and deletion in "HFC-6000 Safety System Topical Report," PP901-000-01 Revision C (Non-Proprietary) dated November 19, 2008 which was transmitted by letter dated March 19, 2008 from Doosan HF Controls Corporation to the U. S. Nuclear Regulatory Commission. The Proprietary version ("Proprietary" marked on each page) was previously transmitted by letter dated March 5, 2008 from Doosan HF Controls Corporation to the U. S. Nuclear Regulatory Commission.

Proprietary Information Notice

Transmitted by letter dated March 05, 2008 from Doosan-HF Controls Corporation to the US Nuclear Regulatory Commission was a Proprietary version of the Topical Report, "HFC-6000 Safety System Topical Report" furnished to the NRC in connection with a request for generic review and approval. Transmitted by letter dated March 19, 2008 from Doosan-HF Controls Corporation to the US Nuclear Regulatory Commission is a Non-Proprietary version of the same Topical Report furnished to the NRC to comply with Commission policy.

In order to conform to the requirements of 10 CFR 2.390 of the Commission's regulations concerning the protection of proprietary information so submitted to the NRC, the proprietary version is labeled with the word "Proprietary" on each page and in the Non-Proprietary version, the proprietary information has been bracketed and deleted such that only Non-Proprietary information remains. Since the Proprietary information contains only one type of proprietary information which is confidential commercial whose use by a competitor would improve his commercial position to the detriment of Doosan HFC corporation; adjacent marking for each deletion would be redundant and an unnecessary burden. The proprietary marking on each page is adequate and is compliant with Section 2.390.