HF Controls

Amendment for HFC-FPGA System of HFC-6000 Safety Platform

RR901-107-10 Rev F

Effective Date: 4 / 3 / 19

Prepared By: Eugene O'Donnell / Yin Guo

Reviewed By: Huaisong Xu

Approved By: Allen Hsu

INFORMATION ONLY

HFC Proprietary

Copyright© 2019 HF Controls Corporation

Revision History

Date	Revision	Author	Changes
2/3/2015	A	Ivan Chow	Submitted to the US NRC
4/5/2015	B1	J Taylor	Addition of HFC-FCPU
1/24/2016	B2	J Taylor	Remove loop controller references
5/27/2016	B	E. O'Donnell	Addition of FCPUX and FPUM2
7/10/17	C	E. O'Donnell	Added detail from EQ results
3/8/18	D	E. O'Donnell	Update of references for NUREG 0800-7
7/28/18	E	E. O'Donnell, Yin Guo	1. Clarify that this HFC-FPGA system is solely using FPGA chips to implement all PCBs in Section 1.0 except Gateway Controller. 2. Add description of FPGA as compared to microprocessors to emphasize the FPGA advantages (Section 5.1). 3. Provide details on the hardware development process in Section 5.2. 4. Section 5.3 updated with references and terminology (e.g. FSM) clarifications. 5. Provide details on the FPGA software development process in Sections 5.4 and 5.5. 6. Add paragraph to emphasize that HFC's QAPM is consistent with 10 CFR Part 50 Appendix B in Section 6.8. 7. Add references to Section 6.9 for clarifying deterministic behavior. 8. Add references to clarify IEEE Std 603 compliance in Section 6.9.3. 9. Add GDC 21 details and references in Section 6.9.5. 10. Reference FMEA for GDC 23 in Section 6.9.5. 11. Expand Section 6.10 to include specifics for defense in depth. 12. Add Section 6.11 Cyber Security details and SDOE. 13. Add Section 7 on tools use and qualification per IEEE 7-4.3.2 guidance. 14. Add Section 9.1 for SCR process.
1/30/2019	F	E. O'Donnell, Yin Guo	1. Revise Section 4.0, 4.1. 2. Delete Section 4.2, 4.3, 4.4. 3. Expand Section 5.1 to include hardware specifics for HFC-FPGA modules. 4. Expand Section 5.3 to include FPGA logic specific for HFC-FPGA modules. 5. Add HFC-FPGA development process to Section 5.5. 6. Expand Section 6.0 to include more technical design detail related with safety system.

			7. Remove several RG related only to plant-specific review. 8. Add details of QA program to Section 6.8 9. Expand Section 8.0 to include more details related with EQ test. 10. Move Section 9.0 to Section 5.88 11. Add ISG section.

Table of Contents

Section	Title	Page
1.0	Purpose and Scope	7
2.0	Terms and Abbreviations	10
2.1	Definitions	10
2.2	Special Terms, Acronyms and Abbreviations	11
3.0	Regulations, Codes, Standards, Guidance and References	14
3.1	NRC Regulations and Guidance	14
3.2	Industry Standards	16
3.3	HFC Technical Documents	18
3.4	HFC-6000 NRC Reviewed Documents	19
3.5	HFC Quality Procedures	19
4.0	HFC-FPGA System Overview	20
4.1	Advantages of HFC-FPGA system used in Safety Applications	22
5.0	HFC-FPGA System Hardware/Software	24
5.1	Hardware Architecture	24
5.1.1	Common Hardware Components	24
5.1.2	Module Specific Components	25
5.1.2.1	System Controller Module	25
5.1.2.2	Input/Output Modules	29
5.1.2.3	HFC-HSIM	33
5.1.2.4	Gateway Controller HFC-FPC08	34
5.1.3	Power Distribution and Chassis	35
5.1.4	Communication Links	35
5.2	Hardware Development Process	37
5.3	FPGA Software Architecture	39
5.3.1	Control FPGA Software Architecture	40
5.3.2	Diagnostic FPGA Software Architecture	45
5.4	FPGA Software Development Process	47
5.5	FPGA Specific Implementation	48
5.6	Application Control	55
5.7	The Adoption of HFC-6000 Product Line Architecural Concepts	55
5.8	HFC Configuration Management	57
6.0	Safety System Design Topics	59
6.1	Centralized Controller Module Characteristics	59
6.2	I/O Module Characteristics	60
6.3	Control/Diagnostic FPGA Characteristics	61
6.4	C-Link	62
6.5	F-Link	63
6.6	G-Link	65
6.7	Deterministic Performance Conclusion	65
6.8	Quality Assurance Program	66
6.9	Regulations, Codes, Standards and Guidance for Digital System Implementation	67
6.9.1	General	67
6.9.2	Compliance with USNRC Documents	67
6.9.3	Compliance with IEEE Standards	79

6.9.4 Other Documents ... 87
6.9.5 CFR and General Design Criteria ... 87
6.10 Defense-In-Depth and Diversity Evaluation Process ... 90
6.10.1 NRC Position 1: ... 91
6.10.1.1 Compliance with Position 1: ... 91
6.10.2 NRC Position 2: ... 91
6.10.2.1 Compliance with Position 2: ... 91
6.10.3 NRC Position 3: ... 91
6.10.3.1 Compliance with Position 3: ... 91
6.11 Cyber Security ... 92
6.11.1 Vulnerability Assessment ... 92
6.11.2 Secure Development and Operational Environment Controls ... 93
6.12 Isolation and Independence ... 93
7.0 Tool Use and Qualification ... 94
7.1 Tool Qualification Methodology ... 94
7.2 Qualification of One-Step ... 95
7.3 Qualification of Other Third Party FPGA Tools ... 97
8.0 Equipment Qualification ... 98
8.1 System Qualification Tests ... 98
8.1.1 Scope ... 98
8.1.2 Equipment Tested ... 99
8.1.3 Safety Functions Tested ... 102
8.1.4 Test Requirements ... 102
8.1.4.1 Test Procedures ... 103
8.1.4.2 Test Personnel ... 104
8.1.4.3 System Operational Stress Conditions ... 104
8.2 System Qualification Test Results ... 106
8.2.1 Prequalification Tests ... 106
8.2.2 Operability Tests ... 106
8.2.3 Prudency Tests ... 107
8.2.4 Qualification Tests ... 108
8.2.4.1 Environmental Stress Qualification Tests ... 109
8.2.4.2 EMI/RFI Qualification Tests ... 110
8.2.4.3 ESD Test ... 110
8.2.4.4 Surge Withstand/EFT/Burst Immunity Test ... 111
8.2.4.5 Seismic Stress Test ... 112
8.2.5 Post Qualification Tests ... 114
8.2.6 Test Results and Conclusion ... 114
9.0 Conclusion ... 115

List of Figures

Number	Title	Page
Figure 1.	HFC-FPGA System Context	8
Figure 2.	Test Specimen Equipment Block Diagrams	22
Figure 3.	Communication Interface of Redundant HFC-FCPU Configuration	27
Figure 4.	HFC-FPGA Controller Watchdog Mechanism	28
Figure 5.	HFC-FPGA I/O Module Configuration Block Diagram	30
Figure 6	HFC-FPGA I/O Module Watchdog Mechanism	31
Figure 7.	HFC-HSIM Design Block Diagram	34
Figure 8.	Typical HFC-FPGA System Communication Arrangement	36
Figure 9.	Hardware Development Process	38
Figure 10.	General Arrangement of FPGAs in Controllers and Modules	40
Figure 11.	Detailed Control FPGA Architecture	41
Figure 12.	Redundancy Interface Block Diagram	43
Figure 13.	G-Link Module Block Diagram	44
Figure 14.	Detailed Diagnostic FPGA Architecture	46
Figure 15.	The Implementation of FPGA as a Subsystem Embedded in the Overall System	47
Figure 16.	V-Model Illustration for FPGA Lifecycle Design & Implementation Process	48
Figure 17.	FPGA Development Process Flow	50
Figure 18.	HFC-FCPU/HFC-FCPUX Block Diagram	60
Figure 19.	Example HFC-FPGA I/O Module Block Diagram	61
Figure 20.	State Diagram for Token-passing Mechanism	65
Figure 21.	Two Acceptable Methods for Tool Qualification	95
Figure 22.	Additional Approach to Ensure the Correctness of FPGA One-Step	97
Figure 23.	Overall Test Arrangement and Sequence	99
Figure 24.	Environmental Stress Test Profile	109
Figure 25.	Seismic Test Spectrum	113

List of Tables

Number	Title	Page
Table 1.	Qualification Modules	20
Table 2.	List of Common Library Modules	42
Table 3.	List of Logic Library Modules	45
Table 4.	Token-Passing Protocol Comparison	63
Table 5.	Reliability and Availability Results	81
Table 6.	Qualification Test Specimen Items	100
Table 7.	FPGA Type and Quantity	102
Table 8.	Burst of Events Points	108

1.0 PURPOSE AND SCOPE

The HFC-FPGA system (at times referred to as HFC-FPGA for short) is the current generation of the HFC-6000 product line, which is based on FPGA hardware architecture rather than microprocessors or other forms of microcontrollers. Depending on the needs and complexity of a particular application, this version of the HFC-6000 could be implemented using one of three design architectures:

- A central controller architecture in which a redundant FPGA-based controller is linked to individual HFC-FPGA I/O modules.
- A distributed loop controller architecture in which each FPGA-based I/O module executes its own portion of application code.
- A triple redundant controller configuration with each FPGA-based controller linked to an identical set of HFC-FPGA I/O modules (Triple Modular Redundant (TMR) configuration).

The present amendment to the HFC-6000 Safety Platform covers only the central controller architecture. The resulting HFC-FPGA system is intended to operate as an essentially autonomous controller for a single safety train within a larger control system for a nuclear power plant.

The HFC-FPGA system and modules addressed in this amendment were designed to be an expansion of the existing HFC-6000 system's capabilities while adhering to the same design principles. However, HFC-FPGA system utilizes FPGA technology entirely, except the Gateway Controller HFC-FPC08. In other words, all PCBs include controller and I/O modules, except the Gateway Controller HFC-FPC08, are implemented by utilizing FPGA technology solely and there is neither microprocessor nor Digital Signal Processor (DSP) applications in the HFC-FPGA modules. Table 7 states what FPGA chips were used on each HFC-FPGA module in detail. The HFC-FPC08 utilizes a combination of FPGA and microprocessor technology, as described in DS901-001-99 FPC08 G-Link Gateway Software Design Specification and Section 5.1.2.4.

The HFC-FPGA system, at times referred to as the HFC-FPGA platform, was conceived and designed to provide the same capabilities as the original HFC-6000 system using a different hardware and software configuration. With these expanded options for configuration, HFC intends to be able to provide an FPGA or microprocessor solution to NPPs that will enhance diversity of the protection system. This diversity will be assessed on the plant level.

The equipment classified as modules in the HFC-FPGA system are listed in Table 1. These modules were assembled in a representative test specimen designated as the VV0115 Test Specimen for all equipment qualification. Only the items in Table 1 are within the scope of this amendment. All other equipment used within the VV0115 Test Specimen as listed in Table 6 is support equipment selected to simulate a generic installation. The HFC-FPGA platform is designed for use as one or more divisions in an NPP, as shown in Figure 1.

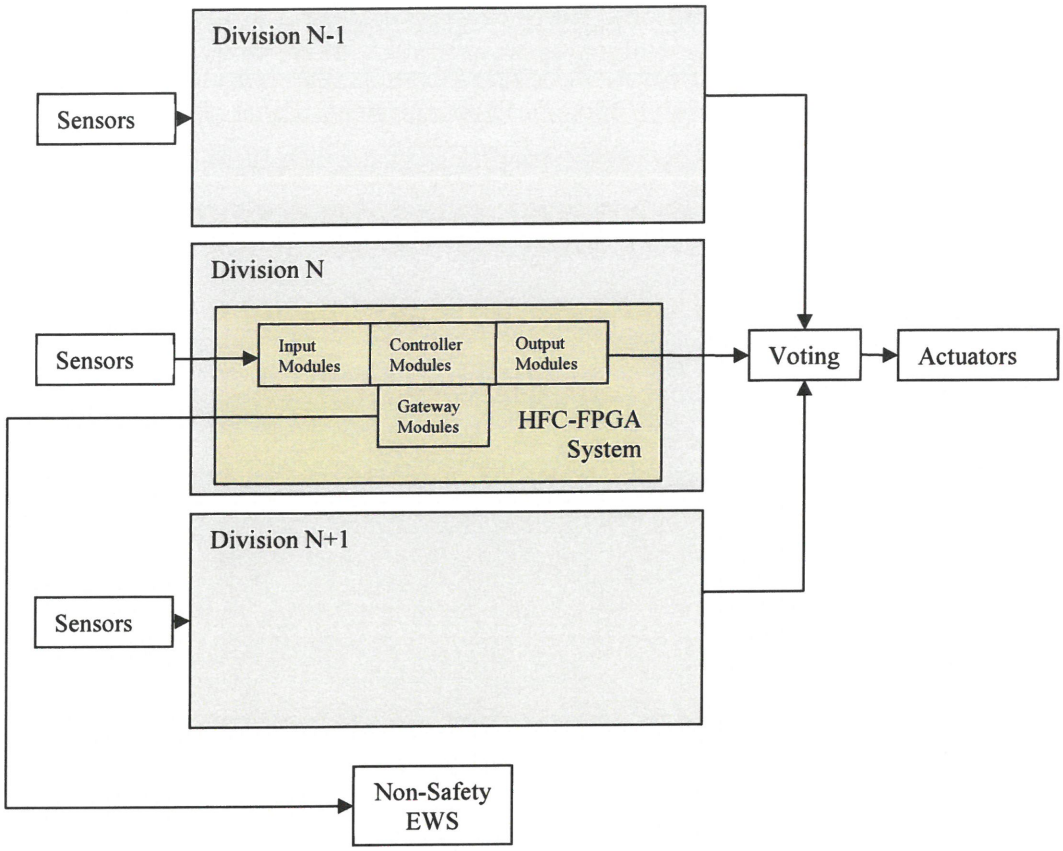

Figure 1. HFC-FPGA System Context

The HFC-FPGA system is designed to provide I/O processing and control in NPP safety systems, functioning as an independent and isolated division. The scope of this amendment is the modules and function of the HFC-FPGA system in a generic single-division configuration as shown in Figure 1. The use of the HFC-FPGA system in conjunction with other divisions will be evaluated on a plant-specific basis.

The development process used in the design and implementation of the HFC-FPGA system were similar to those used to develop the HFC-6000 system, with updates and enhancements made to the development process to reflect updates in industry standards, regulatory guidance, and FPGA-specific tasks and design requirements. The hardware development process is detailed in Section 5.2, and the FPGA development process is detailed in Section 5.4.

The qualification program for these modules was performed using the regulations, codes, standards, and guidance as discussed in Section 8.0 that are applicable to the design and qualification of digital safety systems and the scope of this amendment. This qualification program was performed using the requirements and test conditions from EPRI TR-107330 as a generic basis for qualification testing acceptance criteria. VV0115 Test Specimen was designed to incorporate all qualifying modules and exercise them in a manner described in EPRI TR-107330 in the same manner of the original HFC-6000 qualification system. A Test Specimen Application Program was defined and produced to exercise the VV0115

Test Specimen and monitor the system's performance before, during, and after qualification testing. The full set of hardware that was assembled to make the VV0115 Test Specimen is detailed in Table 6. The plant-specific FPGA logic for application function will be developed in accordance with the provisions of Branch Technical Position 7-14 to qualify this FPGA logic on plant-specific basis.

Throughout the design process, the HFC-FPGA system was analyzed and tested to ensure compliance with applicable industry and government regulations. Details of compliance with each standard and regulation are listed in Section 6.9.

HFC requests that the NRC review the HFC–FPGA modules as described in this amendment. This includes the modules as described in Table 1 of 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, and the modules' relationship with the qualified HFC-6000 system.

2.0 TERMS AND ABBREVIATIONS

2.1 DEFINITIONS

Acceptance Test	Formal test conducted to determine if a system satisfies its acceptance criteria and to enable a customer to assess the acceptability of the system.
Failure Modes and Effects Analysis (FMEA)	A systematic evaluation of component responses to a postulated failure condition.
HFC-6000	Control system line produced by HF Controls. Initial modules of this control system line are qualified by the USNRC per ML110831014, and more have been added to the list of qualified modules via amendments.
HFC-FCPU	HFC-FCPU is the HFC-FPGA system controller, which uses FPGA chips (IGLOO2 M2GL050, see Table 2 of VV901-300-10) to perform the overall operating function of the system. This controller module provides onboard I/O functions.
HFC-FCPUX	HFC-FCPUX is the HFC-FPGA system controller, which uses FPGA chips (IGLOO2 M2GL150, see Table 2 of VV901-300-10) to perform the overall operating function of the system.
HFC-FPGA	Shorthand name for the HFC-FPGA system, and FPGA versions of modules included in the HFC-6000 system.
Lifecycle Phase	Any period during a project that may be characterized by a primary type of design activity being conducted. Different phases may overlap; for V&V purposes, no phase is complete until its development products in the phase are verified fully and/or validated.
Operability Tests	A set of tests performed per Section 5.3 of EPRI TR-107330.
Prudency Tests	A set of tests performed per Section 5.4 of EPRI TR-107330.
Test Specimen	A specific combination of hardware and software components to be subjected to specified test conditions.
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 lifecycle phase, or it may encompass an entire project.
VV0115	Project designation for the HFC-6000 Amendment for the HFC-FPGA system.

2.2 SPECIAL TERMS, ACRONYMS AND ABBREVIATIONS

A/D	Analog-to-Digital
AC	Alternating Current
AI	Analog Input
ANSI	American National Standards Institute
AO	Analog Output
ASME	American Society of Mechanical Engineers
ASTS	Automatic Seismic Trip System
ATWS	Anticipated Transients Without Scram
AUX	Auxiliary
BOE	Burst of Events
BOM	Bill-of-Materials
BTP	Branch Technical Position
C	Celsius/Centigrade
CAD	Computer-Aided Design
CFR	Code of Federal Regulations
C-Link	Communication link between HFC-FPGA Gateways and EWS implemented with a token-passing protocol
CLB	Configurable Logic Block
CPU	Central Processing Unit
CQ4	HFC Analog Algorithm
CRC	Cyclic Redundancy Check
D/A	Digital-to-Analog
DDB	Dynamic Database
DI	Digital Input
DIP	Dual In-line Package
DO	Digital Output
DSP	Digital Signal Processor
DUT	Design Under Test
EFT	Electric Fast Transient
EMI	Electro-Magnetic Interference
ELPC	Ethernet Low Pin Count Connection Interface
EPRI	Electric Power Research Institute
EPROM	Erasable Programmable Read-Only Memory
EQ	Equipment Qualification
ESD	Electrostatic Discharge
ESFAS	Engineered Safety Features Actuation System
EWS	Engineering Workstation
F-Link	FPGA communication link that uses the token-passing protocol developed for the C-Link and backplane hardware traces developed for the ICL
FPGA	Field Programmable Gate Array

FPU	FPGA Processing Unit
FSM	Finite State Machine
G-Link	Dedicated communication link between the HFC-FCPU/HFC-FCPUX and the Communication Gateway
GDC	General Design Criteria
HAS	Historical Archiving System
HDL	Hardware Description Language
HDS	Hardware Design Specification
HFC	HF Controls
HICB	Instrumentation and Control Branch
HPAT	HFC Programmable Automatic Tester
HPI	HFC Peripheral Interface
HRS	Hardware Requirements Specification
HSIM	High Speed Interface Module
Hz	Hertz
I&C	Instrumentation and Control
IAEA	International Atomic Energy Agency
ICL	Intercommunication Link
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
I/O	Input/Output
JTAG	Joint Test Action Group
LAB	Logic Array Block
ms	milli-second
mA	milli-Ampere
Mbps	Megabits per second
MFM	Master-for-a-Moment
MHz	Mega Hertz
MS	Microsoft
MSB	Most Significant Bit
NPP	Nuclear Power Plant
NQA	Nuclear Quality Assurance
NRC	Nuclear Regulatory Commission
OBE	Operating Basis Event
OEM	Original Equipment Manufacturer
PCB	Printed Circuit Board
PLC	Programmable Logic Controller
PLL	Phase Lock Loop
PS	Power Supply
QA	Quality Assurance
QAPM	Quality Assurance Program Manual
QPP	Quality Process Procedure
R&D	Research & Development
RFI	Radio Frequency Interference
RG	Regulatory Guide
RH	Relative Humidity
RIF	Redundancy Interface

RPS	Reactor Protection System
RRS	Required Response Spectrum
RTD	Resistance Temperature Detector
RTL	Register-Transfer Level
RTS	Reactor Trip System
SAR	Safety Analysis Report
SCM	Software Configuration Management
SCR	System Change Request
SE	Safety Evaluation
SER	Safety Evaluation Report
SEU	Single Event Upset
SIL	Software Integrity Level
SOC	System-on-a-chip
SOE	Sequence of Events
SPI	Serial Peripheral Interface
SQL	Structured Query Language
SRP	Standard Review Plan
SRS	Software Requirement Specification
SSE	Safety Shutdown Event
STA	Static Timing Analysis
Std	Standard
TMR	Triple Modular Redundant
TR	Topical Report
TRS	Test Response Spectrum
TSAP	Test Specimen Application Program
TUV	Technischer Überwachungsverein
USNRC	United States Nuclear Regulatory Commission
V&V	Verification & Validation
VGA	Video Graphic Array
VHDL	VHSIC Hardware Description Language
V	Volts
Vrms	Voltage Root Mean Square
WI	Work Instruction

3.0 REGULATIONS, CODES, STANDARDS, GUIDANCE AND REFERENCES

Listed below are the standards, codes, regulatory documents, and guidance which are applicable to the FPGA modules for the process and procedures related to their development lifecycle, installation, operation and maintenance. The accepted topical report, PP901-000-01, provides the conformance details of the HFC-6000 Safety Platform to these codes and standards. Since the development process for the current set of modules did not deviate from the process used for the original qualification of the HFC-6000 Platform, the details of the conformance are not provided in this document. For more information, refer to NRC SE of HFC-6000 Safety Platform, ML110831014, which provides the verification details of HFC-6000 conformance to these codes and standards.

3.1 NRC REGULATIONS AND GUIDANCE

10 CFR Part 21 "Reporting of Defects and Noncompliance"

10 CFR Part 50, App A "General Design Criteria For Nuclear Power Plants"

10 CFR Part 50, App B "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants"

DI&C-ISG-04 "Highly-Integrated Control Rooms—Communications Issues", Rev. 1, 2009

DI&C-ISG-06 "Licensing Process", Rev. 2, 2018

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

NUREG/CR-7006 "Review Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems"

NUREG-0800 "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants"

BTP 7-1 "Guidance on Isolation of Low-Pressure Systems from the High-Pressure Reactor Coolant System", Rev. 6, 2016

BTP 7-2 "Guidance on Requirements of Motor-Operated Valves in the Emergency Core Cooling System Accumulator Lines", Rev. 6, 2016

BTP 7-3 "Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service", Rev. 6, 2016

BTP 7-4 "Guidance on Design Criteria for Auxiliary Feedwater Systems", Rev. 6, 2016

BTP 7-5 "Guidance on Spurious Withdrawals of Single Control Rods in Pressurized Water Reactors", Rev. 6, 2016

BTP 7-6 "Guidance on Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode" Rev. 6, 2016

BTP 7-8 "Guidance for Application of Regulatory Guide 1.22", Rev. 6, 2016

BTP 7-9	"Guidance on Requirements for Reactor Protection System Anticipatory Trips", Rev. 6, 2016
BTP 7-10	"Guidance on Application of Regulatory Guide 1.97", Rev. 6, 2016
BTP 7-11	"Guidance for Application and Qualification of Isolation Devices", Rev. 6, 2016
BTP 7-12	"Guidance on Establishing and Maintaining Instrument Setpoints", Rev. 6, 2016
BTP 7-13	"Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors", Rev 6, 2016
BTP 7-14	"Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems", Rev. 6, 2016
BTP 7-17	"Guidance on Self-Test and Surveillance Test Provisions", Rev. 6, 2016
BTP 7-18	"Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems", Rev. 6, 2016
BTP 7-19	"Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based I&C Systems", Rev. 7, 2016
BTP 7-21	"Guidance on Digital Computer Real-Time Performance", Rev.6, 2016
RG 1.22	"Periodic Testing of Protection System Actuation Functions", 1972
RG 1.28	"Quality Assurance Program Criteria", 2017
RG 1.29	"Seismic Design Classification", 2007
RG 1.47	"Bypassed and Inoperable Status Indications for Nuclear Power Plant Systems", 2010
RG 1.53	"Application of the Single-Failure Criterion to Safety Systems", 2003
RG 1.62	"Manual Initiation of Protective Actions", 2010
RG 1.75	"Independence of Electrical Safety Systems", 2005
RG 1.100	"Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants", 2009
RG 1.105	"Setpoints for Safety-Related Instrumentation", 1999
RG 1.118	"Periodic Testing of Electric Power and Protection Systems", 1995
RG 1.152	"Criteria for Use of Computers in Safety Systems of Nuclear Power Plants", 2011
RG 1.153	"Criteria for Safety Systems", 1996
RG 1.168	"Verification, Validation, Reviews, and Audits for Digital Computer Software Used In Safety Systems of Nuclear Power Plants", 2013
RG 1.169	"Configuration Management Plans for Digital Computer Software Used In Safety Systems of Nuclear Power Plants", 2013
RG 1.170	"Software Test Documentation for Digital Computer Software Used In Safety Systems of Nuclear Power Plants", 2013

RG 1.171 "Software Unit Testing for Digital Computer Software Used In Safety Systems of Nuclear Power Plants", 2013

RG 1.172 "Software Requirements Specifications for Digital Computer Software and Complex Electronics Used In Safety Systems of Nuclear Power Plants", 2013

RG 1.173 "Development Software Life Cycle Processes for Digital Computer Software Used In Safety Systems of Nuclear Power Plants", 2013

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

RG 1.209 "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants", 2013

SRM to SECY 93-087 II.Q "Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems"

SRM to SECY 93-087 II.T "Control Room Annunciator (Alarm) Reliability"

3.2 INDUSTRY STANDARDS

ASME NQA-1 "Quality Assurance Requirements for Nuclear Facility Applications", 2008, 2012, 2015 with addenda NQA-1a-2009 and NQA-1b-2011

EPRI TR-107330 "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants", December 1996

IAEA NP-T-3.17 "Application of Field Programmable Gate Arrays in Instrumentation and Control Systems of Nuclear Power Plants", 2016

IEC 61000-4-2 "Electrostatic Discharge Immunity Test", Edition 2, 2008

IEC 61000-4-4 "Electrical Fast Transient/Burst Immunity Test", Edition 2, 2011

IEC 61000-4-5 "Surge Immunity Test", Edition 2, 2009

IEC 61000-4-12 "Oscillatory Waves Immunity Test", Edition 2, 2006

IEC 60987 "Nuclear Power Plants - Instrumentation and Control Important to Safety - Hardware Design Requirements for Computer-Based Systems", 2007

IEC 62566 "Nuclear Power Plants – Instrumentation and Control Important To Safety – Development Of HDL-Programmed Integrated Circuits For Systems Performing Category A Functions", 2012

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

IEEE Std 279 "Criteria for Protection Systems for Nuclear Power Generating Stations", 1971

IEEE Std 323	"IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations", 2003
IEEE Std 344	"IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations", 2004
IEEE Std 352	"IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems", 1987
IEEE Std 379	"IEEE Standard Application of Single-Failure Criterion to Nuclear Power Generating Station Safety Systems", 2000
IEEE Std 384	"IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits", 1977
IEEE Std 603	"IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations", 1991
IEEE Std 730	"IEEE Standard for Software Quality Assurance Plans", 1989
IEEE Std 828	"IEEE Standard for Software Configuration Management Plans", 1990
IEEE Std 829	"IEEE Standard for Software and System Test Documentation", 2008
IEEE Std 830	"IEEE Recommended Practice for Software Requirements Specification", 1998
IEEE Std 983	"IEEE Guide for Software Quality Assurance Planning", 1986
IEEE Std 1008	"IEEE Standard for Software Unit Testing", 1987
IEEE Std 1012	"IEEE Standard for Software Verification and Validation", 2004
IEEE Std 1012	"IEEE Standard for System and Software Verification and Validation", 2012
IEEE Std 1016	"IEEE Standard for Information Technology--System Design--Software Design Descriptions", 2009
IEEE Std 1042	"IEEE Guide to Software Configuration Management", 1987
IEEE Std 1074	"IEEE Standard for Developing a Software Project Life Cycle Process", 2006
IEEE Std 1228	"IEEE Standard for Software Safety Plans", 1994
IEEE Std 1364	"IEEE Standard for Verilog Hardware Description Language", 2001
ISO 9001:2015	"Quality Management Systems - Requirements"
MIL-STD-461E	"Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment"
NIST 800-53	"Security and Privacy Controls for Federal Information Systems and Organizations", 2013
NIST 800-82	"Guide to Industrial Control Systems (ICS) Security", 2015

3.3 HFC TECHNICAL DOCUMENTS

DS001-007-01	HFC-6000 FPGA System Module Design Specification
DS001-007-02	HFC-6000 FPGA System IP Core Design Description
DS001-007-03	HFC-FPGA Controller Logic Library Component Design Description
DS001-007-04	HFC-FCPU FPGA Software Design Specification
DS901-001-54	HFC-FPUD Hardware Design Specification
DS901-001-64	HFC-FCPUX FPGA Software Design Specification
DS901-001-70	HFC-FPUA Hardware Design Specification
DS901-001-71	HFC-FPUL Hardware Design Specification
DS901-001-72	HFC-FPUAO Hardware Design Specification
DS901-001-73	HFC-FPUM Hardware Design Specification
DS901-001-74	HFC-FCPU Hardware Design Specification
DS901-001-81	HFC-6000 FPGA Platform Diagnostic Design Specification
DS901-001-91	F-Link and G-Link Protocol Design Specification
DS901-002-18	HFC-FCPUX Hardware Design Specification
DS901-002-19	HFC-FPUM2 Hardware Design Specification
DS901-001-20	HFC-HSIM Hardware Design Specification
DS901-000-81	HFC-FPC08 Hardware Design Specification
DS901-003-01	HFC-FPUD FPGA Design Specification
DS901-003-02	HFC-FPUA FPGA Design Specification
DS901-003-03	HFC-FPUL FPGA Design Specification
DS901-003-04	HFC-FPUAO FPGA Design Specification
DS901-003-05	HFC-FPUM FPGA Design Specification
DS901-001-25	HFC-HSIM FPGA Design Specification
DS901-001-99	HFC-FPC08 G-Link Gateway Software Design Specification
ETL Certificate of Test 13999: Environmental Stress Test	
ETL Certificate of Test 14149: Seismic Qualification Test Report	
PP901-000-01	HFC-6000 System Topical Report
PR037435	NTS EMI/RFI Test Report for TP901-302-03, -04, -05
RR901-107-01	FMEA for the FPGA Controllers of HFC-6000 Safety Platform
RR901-107-02	HFC-6000 Reliability and Availability Report for FPGA I/O and Controller Modules
TP901-115-01	VV0115 Qualification Operability Test Procedure
TP901-115-02	VV0115 Qualification Prudency Test Procedure

TP901-115-05	VV0115 Integration (Set-up and Check-out) Test Procedure
TP901-115-06	VV0115 TSAP Validation Test Procedure
TP901-200-01	EPRI TR-107330 Burn-In Test Procedures
TP901-302-02	VV0115 Qualification Environmental Stress Test Procedure
TP901-302-03	VV0115 Qualification EMI RFI Test Procedure
TP901-302-04	VV0115 Surge Withstand Test Procedure
TP901-302-05	VV0115 Electrostatic Discharge Withstand Test Procedure
TP901-302-06	VV0115 Qualification Seismic Test Procedure
TR901-302-01	HFC-FPGA Control System of HFC-6000 Safety Platform Qualification Test Report
VV901-115-09	NRC DI&C ISG-06 Requirements Compliance Traceability Matrix for HFC-FPGA Controller
VV901-117-09	HFC-6000 FPGA Controller Design Phase V&V Task Report
VV901-300-09	VV0115 Qualification Master Test Plan
VV901-300-10	VV0115 FPGA Test Specimen Design Description

3.4 HFC-6000 NRC REVIEWED DOCUMENTS

ML110831014	NRC Safety Evaluation Report of HFC-6000 Safety Platform

3.5 HFC QUALITY PROCEDURES

Quality Assurance Program Manual

QPP 3.1 Design Control

WI-ENG-101	Hardware Development
WI-ENG-103	HDL Coding Standard
WI-ENG-104	Development of Hardware Requirements Specifications
WI-ENG-108	FPGA Development Process
WI-ENG-203	Development of Software/Firmware Design Specifications
WI-ENG-812	System Change Request (SCR) Procedure
WI-VV-201	Project Verification and Validation Procedures

4.0 HFC-FPGA SYSTEM OVERVIEW

This section provides an overview of the HFC-FPGA nuclear safety I&C platform. It includes various I/O, communication, power supply and controller modules and chassis. Refer Section 5.0 for module specific hardware and FPGA logic information.

The HFC-FPGA platform is the FPGA version of HFC-6000 platform, which targets safety-related and important-to-safety application in nuclear power plants. The HFC-FPGA platform was designed by following applicable nuclear regulatory design guidelines, development process and lifecycle to meet regulatory requirements for safety system applications, which include component quality, hardware and software qualification, redundancy, fault tolerance, deterministic performance, isolation and independence.

The HFC-FPGA system consists of a set of PCBs using the HFC-6000 form factor and the I/O connector arrangement so that any HFC-FPGA module can be inserted into any I/O slot of an HFC-6000 expansion rack. The complete set of HFC-FPGA modules includes controllers, I/O modules, the HFC-HSIM F-Link module, and Gateway module as listed in Table 1.

Table 1. Qualification Modules

Part Number	Module Name	Description
[	HFC-FPUD01	FPU I/O Module for 16 DI Channels and 16 DO Channels
	HFC-FPUD02	FPU I/O Module for 32 DI Channels
	HFC-FPUA01	FPU I/O Module for 16 4- to 20-mA AI Channels
	HFC-FPUAO	FPU I/O Module for 8 4- to 20-mA AO Channels
	HFC-FPUL	FPU I/O Module for 8 AI Channels for Type E Thermocouples
	HFC-FPUM	FPU I/O Module for 8 AI Channels for 100-Ohm Platinum RTDs
	HFC-FPUM2	FPU I/O Module for 8 AI Channels for 100-Ohm Platinum RTDs (designed for a higher input accuracy)
	HFC-FCPU	FPGA Controller Module for the HFC-FPGA system with onboard I/O function
	HFC-FCPUX	FPGA Controller Module for the HFC-FPGA system
	HFC-HSIM	F-Link High Speed Interface Module
]	HFC-FPC08	Communication Gateway Controller Without VGA

Figure 2 illustrates a typical arrangement of HFC-FPGA system: a test specimen which was created from the HFC-FPGA modules to support development of the present amendment to the NRC SE-approved HFC-6000 safety platform. This test specimen consisted of two expansion racks with one or more of each of the modules listed in Table 1. The I/O modules provide the hardware interface to field sensors and controlled field

devices and are implemented by different types of I/O printed circuit boards. The I/O modules communicate with the controller module via RS-485 traces on the backplane of the HFC-6000 rack using HFC proprietary token-passing protocol originally developed for the C-Link. This communication link is designated as F-Link. System controllers, HFC-FCPU and HFC-FCPUX, support the execution of FPGA application logic, I/O scan cycles and communication with Gateway controller. A redundant configuration of system controller includes two HFC-FCPU/HFC-FCPUX controller boards which communicate with each other via an additional interface called Redundancy InterFace (RIF). Gateway controller HFC-FPC08 broadcasts the necessary operation status to the overall control system via C-Link networks, which has been previously qualified. Controller module HFC-FCPU/HFC-FCPUX communicates with Gateway controller via a network designated as G-Link. G-Link is implemented via the redundant RS-485 traces on the backplane of the HFC-6000 rack using HFC proprietary token-passing C-Link protocol. As with the qualified modules from the HFC-6000 system, all modules except Gateway controller HFC-FPC08 in the HFC-FPGA system only communicate with plant equipment via I/O interfaces. Modules for qualification addressed in this amendment are located in the labeled green box in Figure 2. The following additional equipment is included to supply operating power and communication connectivity:

- Power supply rack: power supply rack is located at bottom of the test specimen and contains two sets of 24 VDC power supplies (PS);

- I/O simulator rack: I/O simulator rack is referred to as the HPAT (HFC Programmable Automated Tester), which consists of a non-redundant HFC-FPC08 controller and HFC-6000 I/O rack with the HFC-6000 DSP series card types. It provides hardware and software components needed to support Sequence of Events (SOE) logging and closed-loop testing of several test specimen functions;

- Network hub: network hub is located at the top of the test specimen and provides communication connectivity for C-Link.

The additional equipment is excluded from the scope of the present amendment, thus is not listed in Table 1. Detailed information about the additional equipment can be found in the document VV901-300-10, VV0115 FPGA Test Specimen Design Description.

[

]

Figure 2. Test Specimen Equipment Block Diagrams

4.1 ADVANTAGES OF HFC-FPGA SYSTEM USED IN SAFETY APPLICATIONS

With the technology development, FPGAs have evolved from the simple glue logic chips at its inception to the integration of millions of logic gates now that can run at frequencies of hundreds of megahertz. In the nuclear I&C field, FPGAs have adequate capabilities for

most digital I&C applications in NPPs. Features of the FPGA technology can improve the reliability, safety, maintainability, and performance of NPP I&C systems, which have attracted plants gradually to adopt FPGA-based systems. With the FPGA technology, it is also possible to improve the diversity and reduce the system-level common cause failure. With these benefits in mind, HFC developed the HFC-FPGA product line by adopting the FPGA technology with the same system design concept as the original microprocessor-centric HFC-6000 product line. Major advantages of HFC-FPGA are briefly discussed as follows:

First of all, the HFC-FPGA system realizes the true parallel task execution to improve the system availability. Unlike microprocessors, functions performed by HFC-FPGA do not have to compete for the same resources and can be processed simultaneously. Each independent processing task is assigned to a dedicated section in the FPGA chip and can run parallel with other tasks. For example, self-monitoring and diagnostic functions in HFC-FPGA are separated from main safety functions, so that a postulated failure of the self-monitoring and diagnostic functions will not prevent the correct execution of main safety I&C functions. Vice versa, failure of the main safety I&C functions will not impact self-monitoring and diagnostic functions and failure of the main safety I&C functions will be detected and reported by self-monitoring and diagnostic functions. The ability to segregate functions in HFC-FPGA makes it easier to determine failure modes and perform testing.

Secondly, the HFC-FPGA system improves the system reliability benefiting from the simplicity of the FPGA technology. During the development of HFC-FPGA, measures have been taken to avoid unnecessary complexity. The HFC-FPGA system reduces the hardware complexity with less hardware components and interconnections than the microprocessor-based system. The HFC-FPGA system also reduces the logic complexity without having the operating system used in the microprocessor-based system. The HFC-FPGA system is designed and implemented with independent finite state machines to replace the operating system of the microprocessor-based system. The use of dedicated finite state machines improves the determinism and testability of the logic, which in turn improves the system reliability.

Thirdly, the HFC-FPGA system is less prone to the cyber-attack to have better information safety. The HFC-FPGA system does not contain high-level general purpose software that may be easily subjected to undesired and/or malicious modifications. The Verilog codes in the HFC-FPGA design are synthesized and converted to digital logic gates and interconnections to configure the FPGA chip, which makes it hard to be attacked.

Fourthly, the HFC-FPGA system has better portability with reduced exposure to obsolescence. Using Verilog, a generic hardware description language, the logic can be re-implemented with different FPGA products without a major re-design, which reduces the risk for rapid obsolescence and short lifetime.

These benefits make the HFC-FPGA system an excellent platform choice to implement the safety critical systems in NPPs, such as Reactor Trip System (RTS) and Engineered Safety Features Actuation System (ESFAS).

5.0 HFC-FPGA SYSTEM HARDWARE/SOFTWARE

All of the HFC-FPGA modules covered by this amendment share similar FPGA hardware and software architecture with the exception of the HFC-FPC08 Gateway module. The major differences from one module to the next consist of the following:

- Hardware interface for a particular type of signals from field equipment (24VDC Inputs/Outputs, 4-20 mA Inputs/Outputs, etc.).
- FPGA software modules necessary to exercise the specific type of interface hardware installed.
- Switches or other hardware components required to configure interface options.
- The specific combination of LEDs required to indicate status of the interface hardware.
- HFC-FPGA I/O modules and the HSIM module have FPGA hardware and software to support communication only via the F-Link. HFC-FCPU and HFC-FCPUX controller modules have three communication interfaces: F-Link, RIF, and G-Link. FPC08 Gateway modules communicate with the controller modules via G-Link, and outside equipment via C-Link.
- HFC-FPC08 Gateway deviates from the HFC-FPGA system's standard architecture as described in DS901-001-99 FPC08 G-Link Gateway Software Design Specification. As indicated in Section 1.0, the HFC-FPGA system entirely uses FPGA technology except the HFC-FPC08 Gateway, which is not entirely FPGA based and only one FPGA chip is utilized.

5.1 HARDWARE ARCHITECTURE

5.1.1 Common Hardware Components

The hardware designs for all HFC-FPGA module assemblies with the exception of the HFC-FPC08 Gateway module include the following components:

- Dual FPGA configuration where two FPGA modules that communicate with one another via an HFC Peripheral Interface (HPI) link. One FPGA is designated as the "Control FPGA" or "Process FPGA" (In HFC Documentation, "Process FPGA" and "Control FPGA" are synonymous and may be used interchangeably.) and the other FPGA is designated as the "Diagnostic FPGA". The Control and Diagnostic FPGAs are identical hardware components but are programmed differently and have different functional roles in the assembly. The dual FPGA design protects each PCB module from Single Event Upset (SEU) impact to FPGA register via the dual FPGA communicating and comparing diagnostic data test results. (Note: Gateway controller HFC-FPC08 is a microprocessor based board.)

- Two complete sets of switching voltage regulators to produce all required onboard voltage levels. One set of regulators control the operating voltages required by the Control FPGA and all of the components controlled directly by it. The other set controls the voltage levels required by the Diagnostic FPGA. The two sets of power rails are completely isolated from one another.

- Separate voltage monitors for the two sets of power rails. The monitor for the Control FPGA power rails receives operating power from the Diagnostic FPGA power rails and controls a status input to the Diagnostic FPGA. The voltage monitor for the Diagnostic FPGA receives operating power from the Control FPGA power rails and controls a status input to the Control FPGA.

- Reset switch enables manual reset of the assembly. Following a watchdog timeout, actuation of this switch can restart controller operation from cold start.

- Maintenance/Run switch enables manual selection between offline maintenance and normal run modes of operation for the FPGA Controllers.

- Station ID interface enables the FPGAs to read the Station ID number from the hardwired slot location based code on the backplane.

- Redundant RS-485 transceivers constitute the hardware interface to the F-Link.

- One onboard flash memory for each FPGA provides non-volatile storage for configuration parameters required during online operation.

- Board-edge LEDs provide a visual indication of PCB operating status for communication, input/output channel status and error codes.

Hardware design specifics for HFC-FPC08 are detailed in Section 5.1.2.4.

5.1.2 Module Specific Components

This section provides module specific description of the hardware components that make up the HFC-FPGA nuclear safety I&C platform. Each module type has a unique hardware I/O interface appropriate for its function within the control system; however, the I/O section for all board types is electrically isolated from the processing hardware on the board. Refer to the hardware design specification (as provided in Section 3.3) for each board type for detailed information on the I/O interface designs.

5.1.2.1 System Controller Module

The HFC-FPGA safety system provides plant monitoring and control functions, with monitoring and control capabilities. There are two controller modules available for the HFC-FPGA safety system: HFC-FCPU and HFC-FCPUX. Both HFC-FCPU and HFC-FCPUX use FPGA chips to perform the overall operating function of the system. The major differences between these two system controllers are that HFC-FCPUX module is designed to support a large capacity FPGA chip and does not have onboard DI/DO channels, while

there are eight digital output channels and eight digital input channels in the HFC-FCPU. These digital input and output channels on HFC-FCPU are present in the design and VV0115 Test Specimen but their functionality is not evaluated in the scope of this amendment. Despite these differences, they are identical in function and operation within the scope of this amendment as centralized controller modules. In other words, except the Digital I/O function in HFC-FCPU and larger capacity FPGA chip in HFC-FCPUX, application with HFC-FCPU as system controller can be replaced by using HFC-FPCUX as system controller, vice versa and both are operated in the same way. For safety related and important to safety application, the digital I/O function in the HFC-FCPU shall be disabled to avoid introduction of non-qualified interfaces. In this section, description about system controller is based on HFC-FCPU. Due to the identical function and operation feature, the description of system controller module HFC-FCPU below is applicable for both HFC-FCPU and HFC-FCPUX, even just HFC-FCPU is mentioned.

System controller can be configured in a redundant configuration or non-redundant configuration. For redundant configuration, the basic rule is to put the primary controller in even slot and the secondary controller in odd slot. It is recommended to put the two controller modules in the right most adjacent slots and in the upper address rack so that other slots are available for the I/O cards. The station address assignment is fixed for the controller module. The primary controller is in the even slot and has a fixed station address 26-29, the secondary controller is in the odd slot and has a fixed station address 30-33. The most efficient use of the system station address range is to locate the redundant system controller in the upper range of the station address range to allow I/O cards to be placed in lower range. Another reason is that the RIF channel mechanism is designed for adjacent slots. If primary and secondary controller are not installed in the adjacent slots, the RIF channel mechanism would have to accommodate the placement.

For non-redundant configuration, the controller can be in either even or odd slots. For multi-rack system, it is recommended the controller be installed in one of the four right slot as these are unusable for I/O cards. Refer DS901-001-91 F-Link and G-Link Protocol Design Specification for more detail regarding F-Link station address assignment.

The principal functions performed by system controller are:

- Redundant controller operation, system diagnostic, failure detection and failover;
- Execution of FPGA application logic for the specific safety system;
- Communication with HFC-FPGA I/O modules through the F-Link;
- Communication with Gateway controller HFC-FPC08 through the G-Link; and
- For redundant system controller, communication from primary controller to/from secondary controller via RIF.

Figure 3 shows a redundant HFC-FCPU configuration and communication interface.

[

]

Figure 3. Communication Interface of Redundant HFC-FCPU Configuration

In a redundant controller configuration consisting of two HFC-FCPU modules, the primary HFC-FCPU performs the main functions of the system controller while the secondary HFC-FCPU operates as a "hot spare" for the primary HFC-FCPU. RIF is the communication interface between the redundant HFC-FCPU modules that keeps the secondary HFC-FCPU module updated with a current copy of the primary running status. The dynamic data of control functions will be equalized between controllers periodically. If the primary controller fails to receive the status of secondary controller through RIF or the secondary controller does not receive the update from the primary controller within predefined time interval, an alarm will be generated immediately. The failure of RIF communication or secondary controller does not impact the function of primary controller. The controller modules process in parallel and output in different time slots, and failure of the primary controller leaves the I/O modules with data from the secondary controller which is used after a short hysteresis delay. The failover mechanism ensures a smooth transition from primary controller to secondary controller upon error is detected.

The two FPGA chips on HFC-FCPU are intended to work in tandem, processing the same input and output data. The Control FPGA includes digital I/O processing, CQ4 execution, F-Link communication, G-Link communication, RIF communication, diagnostic verification, clock generation and board setting configuration functions. The power initial reset and status monitoring are managed by watchdog function. After the HFC-FCPU board is power initialized, the board configuration module reads the settings from onboard dual in-line package (DIP) switch and station address inputs, then configures itself accordingly. The global clocks are generated by the clock generator. Upon power up or reset, the Diagnostic FPGA waits for synchronization with Control FPGA. It has same boot processes to the Control FPGA after it synchronizes with Control FPGA, but in operation, the Diagnostic FPGA is relegated to monitoring traffic on all communication interfaces and to the verification of control data transmitted. The Diagnostic FPGA controls the F-Link RS-485 transmit enable signal. The Diagnostic FPGA also controls the G-Link RS-

485 transmit enable signal. For any diagnostic non-conformance, the Diagnostic FPGA will prevent the F-Link and G-Link transmit data packet transmission.

There are three types of watchdog mechanism operation in the system controller module. Figure 4. HFC-FPGA Controller Watchdog Mechanism below illustrates the watchdog mechanism implemented for the HFC-FPGA controller.

[

]

Figure 4. HFC-FPGA Controller Watchdog Mechanism

[

]

[

]

5.1.2.2 Input/Output Modules

The HFC-FPGA I/O module provides signal-level interface to the equipment and devices which are being monitored or controlled. HFC-FPGA I/O modules covered in this amendment include

- HFC-FPUD01,
- HFC-FPUD02,
- HFC-FPUA01,
- HFC-FPUAO,
- HFC-FPUL,
- HFC-FPUM,
- HFC-FPUM2.

The major functions performed by the HFC-FPGA I/O modules are:

- Measuring input signals or setting output signals;
- Monitoring data being sent by other F-Link modules;
- Communication with HFC-FPGA system controller through F-Link;
- Self-Diagnostic functions.

An HFC-FPGA I/O module with input channels converts the input signal for each channel into input data, and broadcasts these data over F-Link at regular intervals. An HFC-FPGA I/O module having output channels filters digital data broadcasting over F-Link from system controller at regular intervals and uses this data to control each output point.

Common features of all HFC-FPGA I/O modules are as follows:

- Dual FPGA architecture;
- Dedicated SPI Flash for each FPGA;
- FPGA based intelligent module diagnostics and self-diagnostic capabilities;
- Power on reset circuitry with onboard watchdog timer;
- Redundant power feeds with onboard diode auctioneering and fuse protection;
- Onboard status LED indicators;
- Two independent RS-485 serial interfaces for F-Link communication with the system controller;
- Onboard jumpers and switches for configuration options;
- I/O signal conditioning;
- Two card-edge connectors (P1 and P2) mate with HFC-6000 expansion chassis backplane connectors. Signal assignments for P1 are identical for all HFC-FPGA I/O modules, so that any module can be inserted in any I/O slot of an HFC-6000 expansion chassis. The P2 connector for each I/O module uses the same hardware,

but signal assignments are unique for each module type;

- Onboard hardware watchdog timer triggers reset on response to FPGA's timeout condition.

Figure 5 illustrates the generic HFC-FPGA I/O card FPGA arrangement. Each HFC-FPGA I/O module supports communication with the system controller via the F-Link. The Control FPGA is the main processing element and has the ability to communicate on the F-Link. The Diagnostic FPGA, given the same input data with Control FPGA, monitors the Control FPGA function and provides feedback to the Control FPGA. Each FPGA has a SPI Flash interface. The SPI Flash is programmed with an HFC tool prior to installing in the HFC-FPGA system. The data in the SPI flash represents the configuration data and prepares the HFC-FPGA I/O module for operation. During power up, the contents of the SPI flash are verified and compared with each other. The contents of the both SPI Flash must be identical as failing the compare test prevents the HFC-FPGA I/O module from booting. HFC Peripheral Interface (HPI), shown in Figure 5, provides a diagnostic data pathway between Control and Diagnostic FPGA. Each I/O module has two transceivers that are connected to each redundant F-Link trace.

[

]

Figure 5. HFC-FPGA I/O Module Configuration Block Diagram

Compared with HFC-FPGA controller module, there are only two types of watchdog mechanism operation in the HFC-FPGA I/O module due to that there is no application processing in the HFC-FPGA I/O modules. Figure 6 HFC-FPGA I/O Module Watchdog Mechanism below illustrates the watchdog mechanism implemented for the HFC-FPGA controller. The mechanism of remaining two watchdog is same as those implemented on the HFC-FPGA controller module.

Figure 6 HFC-FPGA I/O Module Watchdog Mechanism

HFC-FPGA I/O modules are also designed with fail-safe features. The I/O Module fail-safe can be either an input or and output module or combination. Input modules when they enter fail-safe condition, stop sending F-Link data to the controller. There is a delay built in to the transition to fail-safe state so that error information can be transmitted to the controller along with channel data that has questionable status. Output modules that transition to the fail-safe state stop receiving data from the F-Link and updating the output channels according to F-Link payload data transmitted by the controller. Output modules do send ACK/PASS tokens for a delay period before entering the fail-safe state to notify the FPGA controller of the error condition. [

]

Below is a brief introduction of HFC-FPGA I/O module.

5.1.2.2.1 HFC-FPUD01/HFC-FPUD02

The HFC-FPUD Module is a 32-channel digital input and output module that can support two configurations: HFC-FPUD01 supports 16 Form C Relay DO channels and 16 DI channels rated for either 24 VDC or 48 VDC. The HFC-FPUD02 supports 32 DI channels rated for either 24 VDC or 48 VDC.

5.1.2.2.2 HFC-FPUA01

The HFC-FPUA Module is an analog input module designed to support 16 AI channels, and several versions are available. Within the scope of this amendment, only the HFC-FPUA01 version is to be considered for qualification. HFC-FPUA01 is designed to support 16 Channels 4-20 mA analog input with FPGA based 24-bit Analog-to-Digital (A/D) converter with advanced signal conditioning. These 16 channels can be configured for self-

powered or transmitter-powered operation. The input channels are independent, isolated and do not require a common ground. Each input channel has independent A/D converter, and is isolated from every other channel, as well as from the control logic. The onboard per-channel A/D converter samples the input signal and performs analog-to-digital conversion every 20 milliseconds. The circuit component parameter drift is compensated by an online auto calibration function. The over-range and under-range input signals are detected and reported as alarm information for control application.

5.1.2.2.3 HFC-FPUAO

The HFC-FPUAO Module is an analog output module designed to support 8 AO channels. These 8 AO channels operate in the range of 4-20 mA. The 12-bit digital-to-analog (D/A) converter with advanced signal conditioning provides the proper data translation which is stored in the onboard memory. Conversion is performed on all 8 points independently since each channel has its own D/A converter. accuracy Each D/A channel is updated only after Control FPGA and Diagnostic FPGA has verified the final output data. While Control FPGA outputs the D/A data to the D/A device, the Diagnostic FPGA also monitors the final output. The analog output channel can be configured by loading the failsafe mode configuration data from flash memory with one of three failsafe modes during the system failure condition: the high, the low, or with their status held at its current state.

Each analog output channel is isolated from other channel circuit as well as the FPGA control circuit. This isolation reduces ringing and crosstalk and is combined with a conditioned excitation voltage, which provides precise analog levels to the field.

5.1.2.2.4 HFC-FPUL

The HFC-FPUL Module is an analog input module designed to support 8 thermocouple AI channels plus one cold junction channel. These 8 thermocouple AI channels operate to receive signals from Type E thermocouples. The input channels are designed with independent 24-bit A/D converter with advanced signal conditioning, isolated, and do not require a common ground. Each input channel is isolated from onboard relays and from the isolation amplifier.

The onboard per-channel A/D Converter samples the input signal and performs analog-to-digital conversion for every 20 milliseconds. The circuit component parameter drift is compensated by online auto calibration function. The collected channel data is processed with HFC advanced signal conditioning algorithm with compensating the cold junction data reading. The over-range and under-range are detected and reported as alarm information for control application.

5.1.2.2.5 HFC-FPUM/HFC-FPUM2

The HFC-FPUM Module is a precision RTD-measuring module designed to support 8 RTD input channels, which can be configurable for common or isolated operation. These 8 RTD input channels support three ranges: Low (0-50 °C), Medium (0-100 °C), and Wide (0-200 °C). These ranges are selected by changing the configuration of onboard switches.

The HFC-FPUM2 Module is a precision RTD-measuring module designed to support 8 RTD input channels. These 8 RTD input channels support three ranges: Low (0-50 °C), Medium (0-100 °C), and Wide (0-200 °C). These ranges are selected by changing the configuration of onboard switches. This module is similar in function as the HFC-FPUM, but has a different chip set and is designed to provide a higher measurement accuracy.

The accuracy requirements for HFC-FPUM are:

- Range 0 ºC to 50 ºC with accuracy of ±0.20% of full scale (0 ºC to 200 ºC)
- Range 0 ºC to 100 ºC with accuracy of ±0.20% of full scale (0 ºC to 200 ºC)
- Range 0 ºC to 200 ºC with accuracy of ±0.20% of full scale (0 ºC to 200 ºC)

The accuracy requirements for HFC-FPUM2 are:

- Range 0 ºC to 50 ºC with accuracy of ±0.10% of full scale (0 ºC to 100 ºC)
- Range 0 ºC to 100 ºC with accuracy of ±0.10% of full scale (0 ºC to 100 ºC)
- Range 0 ºC to 200 ºC with accuracy of ±0.10% of full scale (0 ºC to 200 ºC)

Similar as HFC-FPUL, HFC-FPUM and HFC-FPUM2 onboard per-channel A/D converter samples the input signal and performs analog-to-digital conversion for every 20 milliseconds and the circuit component parameter drift is compensated by online auto calibration function. The collected channel data is processed with HFC advanced signal conditioning algorithm. The over-range and under-range are detected and reported as alarm information for control application.

5.1.2.3 HFC-HSIM

The HFC-HSIM card is designed to function as an HFC-6000 information carrier by transmitting or receiving various bytes of information. HFC-HSIM can be used in both ICL and F-Link network. For HFC-FPGA system, it will be configured in the F-Link mode.

The HFC-HSIM performs the following functions as a transmitter board in HFC-FPGA system:

- Configured with two optical transmission ports;
- Communicate with controllers through F-Link bus;
- Obtain fixed-length data packets from F-Link controllers, serialize data, and transmit the data to an HFC-HSIM receiver card through fiber optic cable from the HFC-HSIMCON;
- Transmit data to HFC-HSIM receivers at 12.5Mbps.

The HFC-HSIM performs the following functions as a receiver board in HFC-FPGA system:

- Configured with two optical reception ports;
- Communicate with controllers through F-Link bus;
- Receive fixed-length data packets from two reception ports at 12.5Mbps;
- Broadcast the received data to F-Link bus.

[

]

Figure 7. HFC-HSIM Design Block Diagram

Figure 7 illustrates the design block diagram of HFC-HSIM. Same as HFC-FPGA controller and HFC-FPGA I/O module, the HFC-HSIM FPGA design is also composed of Control FPGA and Diagnostic FPGA. Both FPGA designs include F-Link, fiber communication, power up management, clock generator. The onboard Control FPGA samples the communication data from F-Link, and serializes the data into intermediate packets for transport to a companion HFC-HSIM configured as an RX. A separate Diagnostic FPGA is used for performing self-diagnostic functions. HFC-HSIM communication supporting equipment is listed in Table 6.

5.1.2.4 Gateway Controller HFC-FPC08

The HFC-FPC08 Gateway module is a gateway communication device that facilitates communication between outside equipment and the centralized controllers. The HFC-FPC08 is a microprocessor based controller. It has one SOC x86 compatible CPU, 4 10/100 Ethernet ports, 4 RS-485 physical links, 1 digital VGA port (optional), 2 USB ports, and one set of keyboard/mouse interface. Depending on application and installed system firmware, the HFC-FPC08 can be used as regular PC, Class-1E grade Flat Panel Display/Controller, loop controller, or communication gateway. In the HFC-FPGA Gateway application, 2 Ethernet ports are configured to communicate via C-Link with an external Engineering Workstation, and 2 Ethernet ports that are configured to communicate with a redundant HFC-FPC08 Gateway via ELPC. The module also supports 2 channels that communicate with a redundant pair of centralized controller modules such as the HFC-FCPU or HFC-FCPUX via G-Link.

Compared with other HFC-FPGA modules, the HFC-FPC08 has different hardware design for power rail, voltage regulators and monitors, reset mechanism, user interface (e.g. LED indication, rotary switches). Hardware design for HFC-FPC08 is detailed in DS901-000-81.

To support the gateway communication function, the HFC-FPC08 gateway software contains two categories of functionality: G-Link communication and C-Link broadcast. The G-Link communication firmware sends and receives data to/from the HFC-FPGA controller module HFC-FCPU or HFC-FCPUX, and stores all data broadcast on that channel. The C-Link is a one-way broadcast communication link. The C-Link broadcast

firmware creates C-Link packets containing data received from the G-Link channel, and broadcasts that data on the C-Link network.

5.1.3 Power Distribution and Chassis

Power sources for the HFC-FPGA system are external to the controller hardware. Reference Figure 2 "24V PS" for the location of the power source. Typically, redundant power supplies are installed either at the bottom or the top of the equipment rack, and redundant power lines are connected first to a power panel within the cabinet, from there to one fuse card for each PCB rack in the cabinet, and from the fuse card to its particular PCB rack. The fuse card has separate safety fuses for each power line connected to its PCB rack, and it also provides LEDs to indicate the operability status of each of its power lines. Fuse card functionality is built into each HFC-FPGA backplane.

All power lines configured for a particular rack land at a common power disconnect, and they are routed from that point to each backplane connector via traces on the backplane. Every I/O connector in the rack receives the same combination of redundant power rails, and onboard hardware performs diode auctioneering and voltage regulation. In contrast, digital channels requiring external excitation power receive AUX power from the HFC-FPGA backplane, and these power traces are isolated from everything else on the assembly. Reference Figure 2 "24V AUX PS" for the location of this power source. Analog circuits requiring excitation receive this power from the analog channel on the I/O module.

The power supply modules and racks used in the VV0115 Test Specimen for qualification are identical to those used in the qualified HFC-6000 system. The 19-inch chassis and backplane HFC-BPE01-19 are also identical to those used in the qualified HFC-6000 system addressed in PP901-000-01 and ML110831014. These modules are detailed in Table 6.

5.1.4 Communication Links

All previous implementations of HFC-6000 control systems included two different hardware arrangements for communication: the RS-485-based ICL and token-passing C-Link protocol. The I/O modules covered by this amendment include only the hardware for the RS-485 communication link, which has been designated as the F-Link. The F-Link is a redundant communication link for all of the HFC-FPGA modules (except Gateway HFC-FPC08) installed in an HFC-6000 PCB rack. The hardware implementation of the F-Link consists of redundant RS-485 traces on the backplane. If a particular implementation of the HFC-FPGA system includes multiple remotes, connection between separate remotes is accomplished via the HFC-HSIM module which sends or receives data to/from another HFC-HSIM module via a fiber optic cable. Figure 8 illustrates a typical communication arrangement for each configured module installed in the HFC-FPGA system.

[

]

Figure 8. Typical HFC-FPGA System Communication Arrangement

Each HFC-FPGA I/O module and HFC-FCPU/HFC-FCPUX controller includes redundant onboard RS-485 transceivers designated as F-Link channel 0 and channel 1. Because the F-Link configuration of the hardware has no single communication master controlling all transfers over the link, the poll-response protocol of the ICL has been replaced by the Master-for-a-Moment (MFM) token-passing protocol, similar to the method used for the C-Link. The F-Link protocol employs two parameters to control the sequence of token passing: the station address ID and the link sequence number. For the present implementation, the remote ID and the link sequence number are both determined by the backplane slot number, which is hardwired to each I/O slot in the PCB rack. Consequently, the HFC-FPGA I/O module in slot 1 is Station Address 0, and it is the first one to claim the token. Then the token is passed from module to module in slot number sequence to the last module in the expansion rack. When the last I/O module relinquishes the token, mastership passes back to Station Address 0. The HFC-HSIM module allows for the passing of F-Link information between remotes via fiber optic lines. Refer to DS901-001-91 for detailed information about the F-Link protocol.

Each of the redundant HFC-FCPU and HFC-FCPUX controllers include a serial link called the RIF and an additional RS-485 interface called the G-Link. The RIF controls a dedicated serial communication link between primary and secondary HFC-FCPU/HFC-FCPUX controllers. This link enables the primary HFC-FCPU/HFC-FCPUX to transfer current status data (e.g. logic gates, registers, etc.) to the secondary HFC-FCPU/HFC-FCPUX throughout normal controller operation.

The G-Link is a dedicated communication path between the redundant HFC-FCPU/HFC-FCPUX controllers and the Gateway Controller module. This link enables transfer of overall control status from the HFC-FCPU/HFC-FCPUX to the common C-Link data highway. Similar to F-Link, G-Link is also using token-passing protocol originally developed for the C-Link. Detail design information about G-Link timing, package, and comparison among F-Link, G-Link and C-Link etc. can be found in Table 4. In the scope of this amendment, the Gateway controller is the HFC-FPC08.

5.2 HARDWARE DEVELOPMENT PROCESS

HFC differentiates its projects into two categories: product line development projects and application project. A product line development project consists of those design activities required to create a new HFC product or to modify an existing one. An application project consists of those design activities required to implement a customer-specific application which may incorporate new, modified and/or existing HFC products. The development project of HFC-FPGA platform is a product line development project. As with software development process, hardware development process is planned and implemented. HFC utilized WI-ENG-101, Hardware Development and IEC 60987-2007 for the structure of the development process.

The hardware development starts with the stakeholder's requirements, which are developed into the system requirements. The software and hardware requirements are then allocated using the system requirements. The requirements allocated to hardware are captured in the Hardware Requirements Specification (HRS). Based on the HRS, the Hardware Design Specification (HDS) shall be developed. Next, the printed circuit board schematics are developed. Meantime, a Bill-of-Materials (BOM) are developed and documented. Next, prototyping begins and prototype test procedure(s) are created. Once the prototyping is completed, the PCB is tested per the released procedure(s) with the applicable firmware (FPGA logic to perform operating function) included. With the successful hardware PCB prototyping testing and design review, the PCB schematics are released for production. Any design flaw detected in the testing or review of the to-be-released material results in repeating the development process from possibly as far back as the requirements stage. The manufactured PCB is inspected and accepted. The PCB is then integrated with the FPGA firmware for the formal testing. If the PCB passes the test, it is accepted for the system integration test. Figure 9 shows the hardware development process.

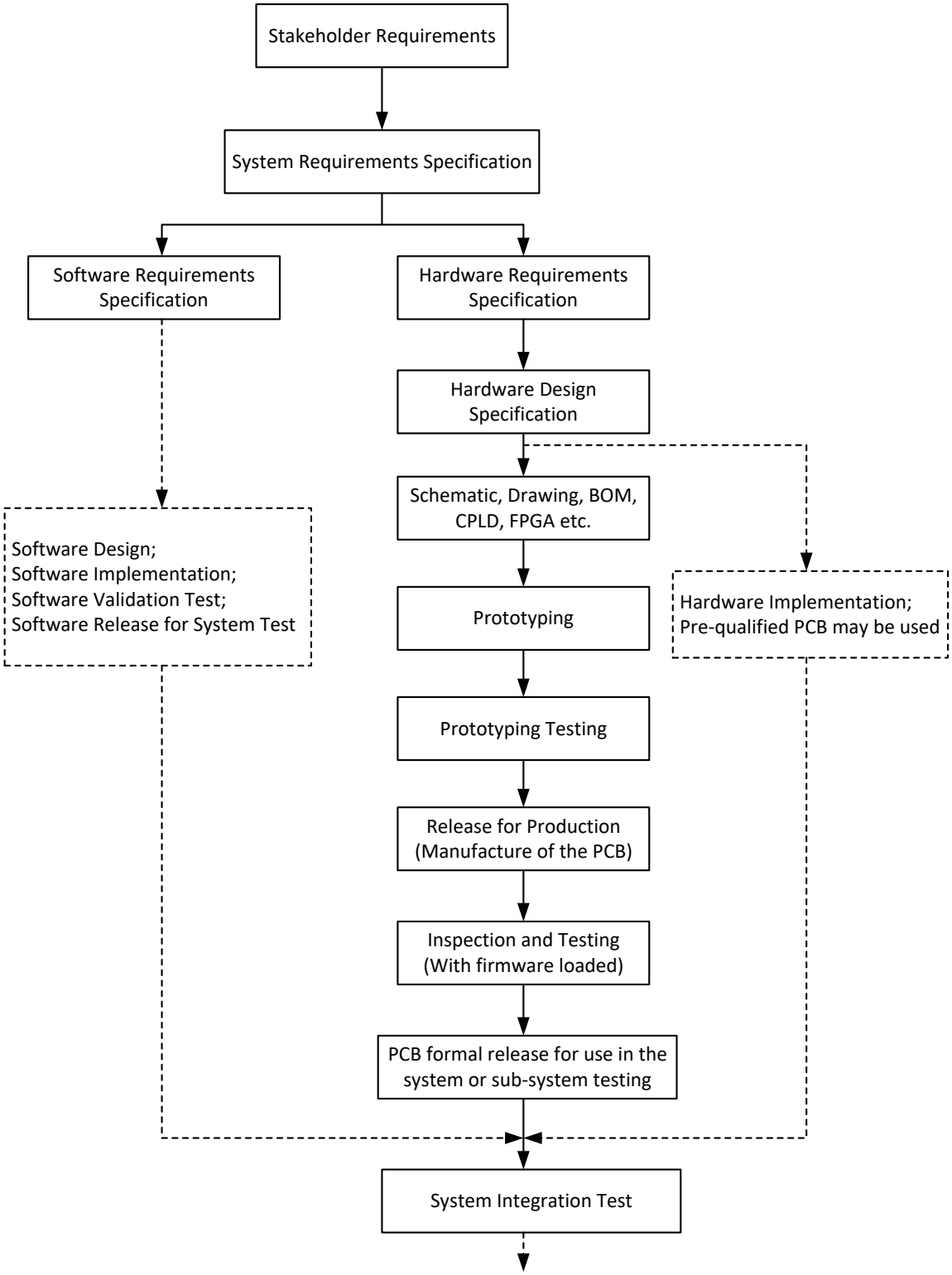

Figure 9. Hardware Development Process

From the hardware development process depicted in Figure 9, the hardware life cycle is essentially similar to the software lifecycle (see Section 5.4), which is detailed in Attachment 7.1 of HFC QPP 3.1 design control and corresponding procedures are developed to implement this development process. However, hardware development

process differs from software development process in the Implementation Phase. The implementation phase activity for hardware is the implementation of the HDS, which leads to the manufacturing of the hardware (PCB in the digital I&C system). The implementation phase of the hardware is complete with the successful testing of the manufactured PCB integrated with software. The specific changes to the development process for FPGA projects are described in WI-ENG-108, FPGA Development Process. WI-ENG-108 follows the guidance from NUREG/CR-7006.

HFC is a 10 CFR Part 50 Appendix B compliant organization and has a QA program in compliance with the ANSI/NQA-1. This quality assurance program is applicable to the HFC-FPGA hardware development process. Detailed information about HFC QA program can be found in HFC Quality Assurance Program Manual (QAPM) and Section 6.8 of this amendment. The HFC QA program is implemented through QPPs, quality plans, process control sheets and work instructions.

5.3 FPGA SOFTWARE ARCHITECTURE

The FPGA software that will be utilized for the safety-related applications of the HFC-FPGA system is divided into two categories: platform software (firmware) and FPGA application logic, both are within the scope of this Topical Report. The platform software is the software that performs, manages, and monitors the overall operating functions and communications. The FPGA application logic is the TSAP.

Figure 10 illustrates the general arrangement of Control FPGA and Diagnostic FPGA in an HFC-FPGA I/O module and an HFC-FPGA controller module. The Control FPGA contains the code that executes all control functions; the Diagnostic FPGA executes the same control functions, and performs diagnostics during execution of those control functions. The two FPGA modules are synchronized, and must remain synchronized with one another in order for any process to be completed without failure. Detection of processing failures is present in each module. Each module can generate error status messages that are included with the data broadcasts to the F-Link. Loss of synchronization between the Control and Diagnostic FPGAs is fatal and will force a fail-safe condition, as discussed in Section 5.1.2.1 and Section 5.1.2.2.

All modules in the Control and Diagnostic FPGAs are written in Verilog and programmed into on-board FPGA chips, which are not alterable by the end user during operation.

Vendor-specific Intellectual Property cores used in HFC-FPGA system include Phase Lock Loop, Hard Memory Blocks and Hardware Multiplier. Refer to DS001-007-02, HFC-6000 FPGA System IP Core Design Description, for the complete list of IP cores used and their descriptions. All the IP core components are generated by Microsemi FPGA design tool Libero.

These vendor-specific Intellectual Property cores were evaluated during the verification and validation process, including software design evaluation, source code and source code documentation evaluation, and software testing at various levels. Based on the evaluation of DS001-007-02 in VV901-117-09, HFC-6000 FPGA Controller Design Phase V&V Task Report, these cores were suitable to be used in the HFC-FPGA system.

[

]

Figure 10. General Arrangement of FPGAs in Controllers and Modules

5.3.1 Control FPGA Software Architecture

The software for the Control FPGA is composed of several sets of software modules each of which performs a distinct function within the controllers. Figure 11 below uses HFC-FCPU as an example to show how these individual functions inside the Control FPGA are connected.

[

]

Figure 11. Detailed Control FPGA Architecture

Each of these sets of software modules is covered in detail by one or more separate publications. The following paragraphs summarize the function(s) performed by each of the software sets and identify the document that provides detailed information.

Common Library Modules. The common library modules are not specifically related to any one processing function. Rather, these modules control common utilities and functions within the software and are used in every HFC-FPGA module. Refer to DS001-007-01 for Table 2 below for brief description of common library modules. Modules used for F-Link communication are tagged with “F-Link” in the Note Column.

Table 2. List of Common Library Modules

Name	Function	Note
[		
		]

F-Link Control Modules. The F-Link control modules create the token-passing protocol for the HFC-FPGA modules. This software has its own top module, and it executes a cyclic operation that runs independently of other processes as long as the **reset** input remains **false**. Some of the F-Link control modules are included with the common library modules as shown in Table 2; the remainders are covered in detail in DS001-007-02.

I/O Interface Control Modules. Because each of the HFC-FPGA modules has a unique hardware interface with the external process under control, the software required to control I/O functions is unique to each PCB assembly. These processes include scanning the hardware I/O interface, data format conversion and validation, and hardware status monitoring. Refer to the FPGA design specification provided in Section 3.3 for each module type for detailed information about these modules.

RIF Control Modules. The RIF hardware and control software exists only on the HFC-FCPU/HFC-FCPUX assemblies. These components control communication between the primary and secondary HFC-FCPU/HFC-FCPUX assemblies.

Figure 12 details how the two HFC-FCPU boards are interconnected to implement the RIF. [

]

equalize the state of both HFC-FCPUs by exchanging data to/from one HFC-FCPU from/to the other. After both HFC-FCPUs have powered-up and are stable, there will be periodically equalization data transfers from the active primary HFC-FCPU to the secondary HFC-FCPU in a predefined time interval. Should the primary HFC-FCPU be removed, the secondary HFC-FCPU is in the same state, ready to take over for the primary. Refer to DS901-001-64 for design description for RIF control modules.

[

]

Figure 12. Redundancy Interface Block Diagram

G-Link Control Modules. The G-Link hardware and control software exists only on the HFC-FCPU/HFC-FCPUX assemblies. The G-Link enables the primary and secondary controller modules to transfer current status for the process under control to the communication Gateway module via redundant RS-485 links. The G-link control module handles all traffic between the physical communication layer and system resources. Figure 13 below shows an overview of G-Link module block diagram. Refer to DS901-001-64 for design description for G-Link Control Modules.

[

]

Figure 13. G-Link Module Block Diagram

Application Logic Processing Modules. The FPGA application logic for HFC-FPGA systems consists of a binary flash memory file, a Verilog logic file, and a platform processing block. The binary file and Verilog file are generated by an HFC software tool called One-Step. One-Step is used during development of a specific application. Processing functions available for specifying the application include: Boolean logic, analog algorithms, and arithmetic operations. The application processing Finite State Machine performs the block operations identified in the flash binary file with the Verilog file during normal operation of the control system. Table 3 below shows a complete list of library modules available in the logic library. Refer to DS001-007-03 for logic library component design description.

Table 3. List of Logic Library Modules

Name	Function
[	
	]

5.3.2 Diagnostic FPGA Software Architecture

The Diagnostic FPGA software controls diagnostic functions for each process controlled by the Control FPGA. Figure 14 below uses HFC-FCPU as an example to show how these individual functions inside the Diagnostic FPGA are connected.

[

]

Figure 14. Detailed Diagnostic FPGA Architecture

The Control and Diagnostic FPGAs are connected to one another by the HPI. Each time the Control FPGA initiates an operation, it informs the Diagnostic FPGA via the HPI. On input modules, the Control and Diagnostic FPGAs receive the same input channel data on the same hardware paths. This input is formed into scan data. This scan data is compared via HPI and sent via F-Link to the controller if no errors are identified. On output modules, when an HFC-FPGA receives data via F-Link, both the Control and the Diagnostic FPGAs receive the same data via the same redundant hardware paths. The two FPGAs then exchange their F-Link data to verify that both receive the same data via F-Link. If there is any discrepancy between the two, then the data is rejected as invalid.

The Diagnostic FPGA maintains a passive status in the operation of the FPU except in the case of failure detection. If the Diagnostic FPGA detects excessive errors in communication, application, or I/O processing, it is capable of taking failsafe actions such as:

1. Resetting the control FPGA.
2. Disabling F-link communication.
3. Generate quality data for any or all I/O channels, strategy to be defined per application.

The Diagnostic FPGA also assists in providing normal run-time error reporting to external resources for monitoring. The diagnostic process validates application logic results and

generates quality data to accompany process data. Quality information generated by communication, I/O pre/post and diagnostic processing is used to dictate application process action or inaction. Error reporting from important system resources is also processed and used to create diagnostic status information for transmission with the F-link payload. Refer to DS901-001-81 for detailed diagnostic design.

5.4 FPGA SOFTWARE DEVELOPMENT PROCESS

The most common FPGA architecture consists of an array of logic blocks (called Configurable Logic Block (CLB), or Logic Array Block (LAB), depending on a vendor), I/O pads, and routing channels. Generally, all the routing channels have the same width (number of wires). Multiple I/O pads may fit into the height of one row or the width of one column in the array.

From the lifecycle process perspective as described in IEEE Std 1074, FPGA is classified as a system element when used in nuclear I&C applications, design and programing are part of the system implementation process in the overall I&C system design. The purpose of the system implementation process is to produce a specified system element implemented as a software and hardware product or service. Within the system implementation process as in the FPGA applications, FPGAs are themselves developed using the full lifecycle process (requirements, architecture and design, implementation, integration, and test). This concept is illustrated in IEEE Std 1012-2012 as shown in Figure 15. The HFC-FPGA design process follows this concept, and in doing so incorporates the core concepts of IEEE Std 1740 into the design process.

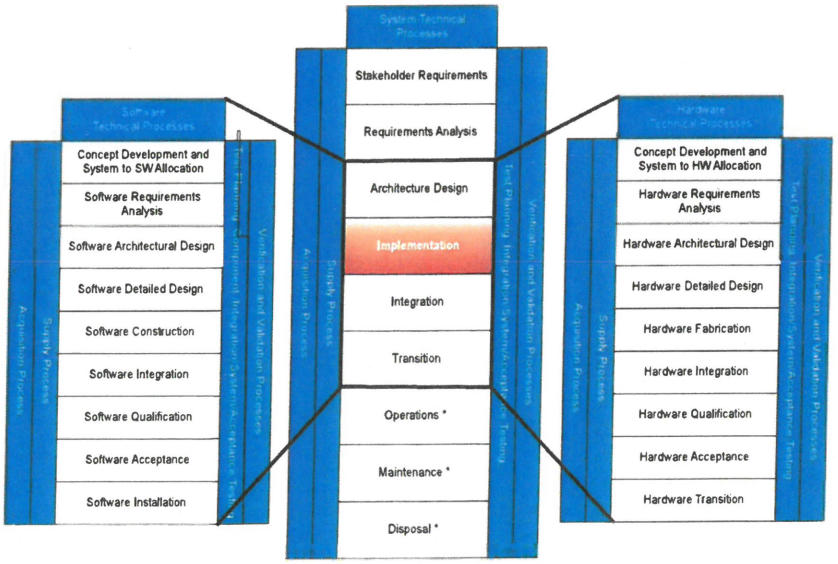

Figure 15. The Implementation of FPGA as a Subsystem Embedded in the Overall System

During the System Implementation Process, the design of FPGA products starts with system of interest functional and performance requirements (from the end user aspect), which are derived from overall safety I&C system requirements. The system of interest

functional and performance requirements are then developed into the FPGA specific requirements as FPGA Requirements Specification. Based on the FPGA Requirements Specification, FPGA architecture and detailed design are developed, which is followed by FPGA implementation.

5.5 FPGA SPECIFIC IMPLEMENTATION

Section 10.2.2 of original HFC-6000 Topical Report PP901-000-01 defines the processes for new software/firmware development in HFC. HFC QPP 3.1 is updated to address the difference between microprocessor and FPGA development process. Work Instruction (WI) WI-ENG-108 is specifically released to provide procedure guidance regarding FPGA development process. The implementation of the FPGA design is what distinguishes FPGAs from the microprocessors. The implementation of the FPGA architecture and design is the process for the FPGA programming, coding, simulation and binary file generation.

Once the FPGA implementation is completed, the FPGA product is integrated into the system for system integration test and subsequently for qualification and acceptance test. Figure 16 shows the FPGA products implementation process following its requirements and design lifecycle phases.

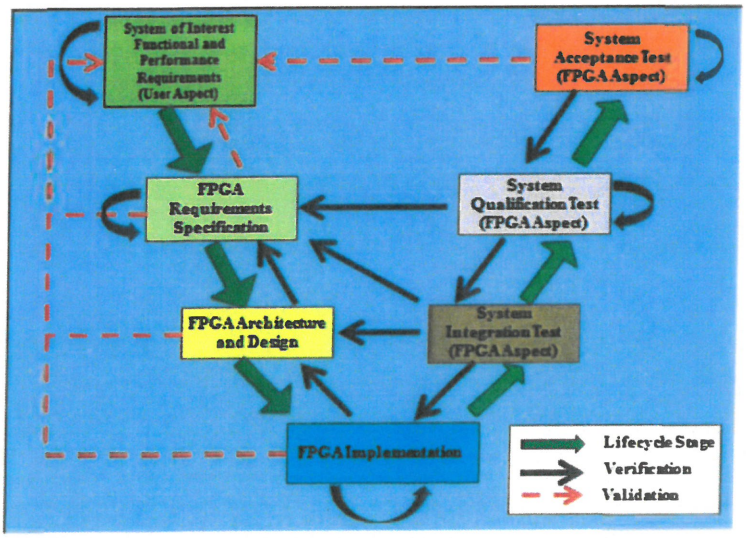

Figure 16. V-Model Illustration for FPGA Lifecycle Design & Implementation Process

During this FPGA implementation process, where the FPGA is being treated as a system of interest element, V&V has to perform in sync with the development to maximize the V&V benefits. The V&V process aims at building quality into FPGA design and ensures correctness of the FPGA implementation and the FPGA end products.

The implementation of FPGA requirements and design consists of the following steps:

- To implement FPGA design, designers use a Hardware Description Language (HDL) or a schematic design. IEC 62566 provides guidance for programming HDL. The HDL form is well suited to work with large structures because it is possible to just specify them textually rather than having to draw every piece by hand.

- Then, using an electronic design automation tool, a technology-mapped netlist is generated. This process is called synthesis, in which the HDL or schematic design is translated to logic gates, memory units, registers and connections.

- The netlist can then be implemented by the FPGA manufacturer's proprietary software to fit to the actual FPGA architecture. This includes translation, map and place-and-route processes. The designer will verify the map, place-and-route results via timing analysis, simulation, and other verification methodologies.

- Once the design and verification process is complete, the programming file is generated (also using the FPGA manufacturer's proprietary software). This file is transferred to the FPGA via a serial interface (JTAG) or to an external memory device like an EPROM.

In a typical design flow, an FPGA application developer will simulate the design at multiple stages throughout the design process. Initially the Register-Transfer Level (RTL) description in VHDL or Verilog is simulated by creating test benches to simulate the system and observe results. Then, after the synthesis engine has mapped the design to a netlist, the netlist is translated to a gate level description where simulation is repeated to confirm the synthesis proceeded without errors. Finally the design is laid out in the FPGA at which point propagation delays can be added and the simulation is run again with these values back-annotated onto the netlist.

During the FPGA development lifecycle process, verification is performed to ensure the results at the end of each phase fulfill the requirements imposed by the previous phase and the internal consistency in each phase. For safety-related FPGA applications development, the design, and HDL programming are reviewed and verified by an independent V&V team.

HFC work instruction WI-ENG-108 details the HFC FPGA Development Process Flow shown in Figure 17 below, left side is R&D only tasks and right side is performed once by R&D and also tested/reviewed by V&V:

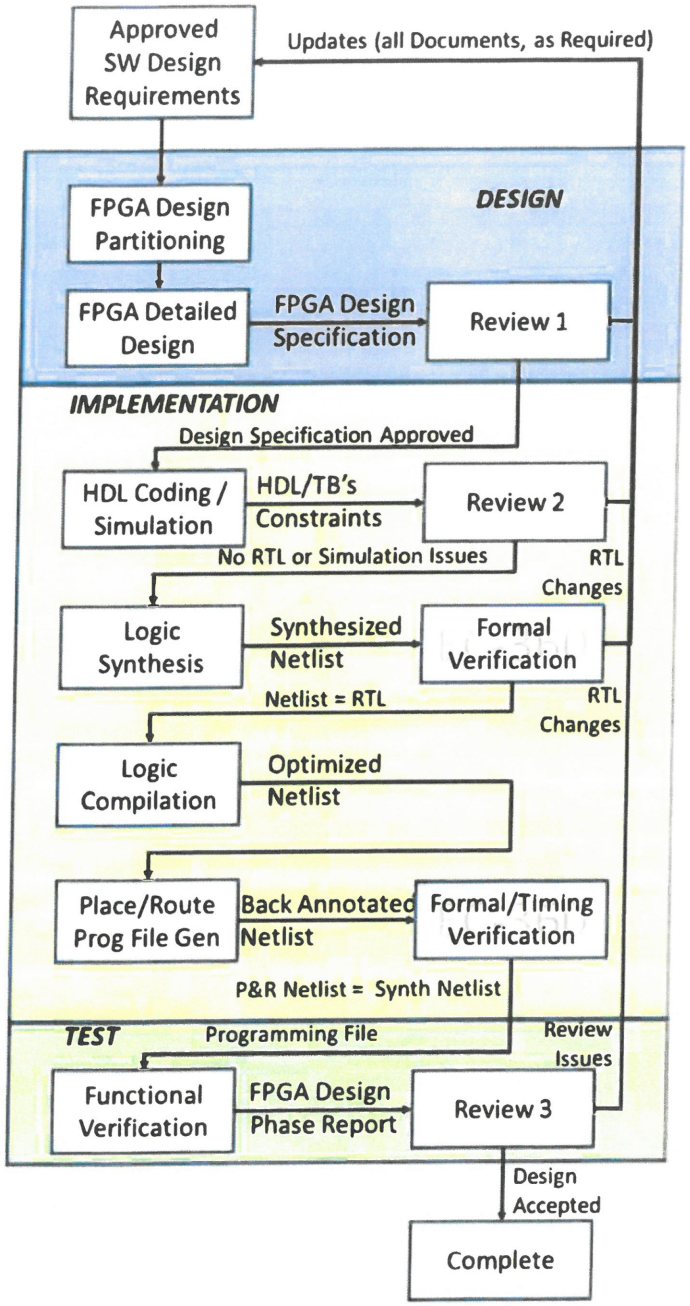

Figure 17. FPGA Development Process Flow

- Software Design Requirements

  The software design requirements document begins with a narrative description of the functional requirements for the FPGA software. Requirements for FPGA's used in safety and safety related equipment shall emphasize reliability and deterministic behavior. This includes the requirement that all code blocks in the design shall operate in a synchronous manner. Requirements need to specify that all error conditions encountered should be detected and reported. These requirements shall

be verifiable and reviewable throughout the FPGA development process. Additional requirements, such as critical timing, power, and board size, may be added to the requirements. FPGA Software requirements can be found in either the Hardware Design Requirements document or the Software Design Requirements documents. In most cases, the Software (RTL) designed interacts directly with the hardware designed on the PCB and therefore including FPGA RTL requirements in the hardware design requirements specification is acceptable. Refer to WI-ENG-104 for more details.

- FPGA Design Partitioning

  Based on the documented requirements from the previous section, the internal design of the FPGA can be divided into functional blocks. These blocks can be classified into the following categories: input blocks, output blocks, and processing blocks. Input and output blocks provide an interface function with an external device. The datasheets for the external device describe the behavior of block, whether it's an input or output or input/output block. Constraints must be developed to manage the input/output timing for these external interfaces. See the user's guide for the toolset being used to create the programming file for more information. Processing blocks use internal FPGA resources to modify data received from external devices through input/output blocks. The processing of data received shall be deterministic and, in most cases, controlled by a Finite-State-Machine (FSM). If possible, functions in input, output, and processing blocks should be divided into smaller blocks in order to achieve complete verification. Functions should be grouped according to a common clock. Where blocks using one clock interface with blocks using a different clock, this should be noted in the FPGA block diagram as a timing domain boundary. Additional circuitry for health monitoring, built-in self-test, redundancy (SEU Mitigation), and observability needs to be considered. The objective is to have a design that has 100% testability. FPGA CPU modules with soft processor cores or hard I/P cores are not allowed in safety or safety related FPGA designs. Design partitioning details shall be documented in the software design specification with an internal FPGA block diagram. The internal FPGA block diagram shall show all external interfaces to the FPGA (in high level detail) and which internal blocks interface to the external interfaces. In addition, a paragraph describing the function of each block shall be included.

  Note: where safety and non-safety functions are intended to reside in the same FPGA, preferred practice is to segment the safety from the non-safety functions into separate FPGA's.

- FPGA Detailed Design

  The objective for detailed design is to define all blocks in the design partitioning, internal FPGA block diagram, in such detail that the design can be coded in HDL by persons not familiar with the architecture. The output of this step is an FPGA software design specification containing the details of each functional block (internal block diagrams, FSM state flows, algorithm details, bus widths, clock boundaries and synchronization, etc.), the details of their interfaces (bus widths,

control signals, etc.), and other information necessary for HDL coding. This detailed design information shall be captured in the Software Design Specification. Refer to WI-ENG-203 for more details.

Note: If in the process of Detailed Design, areas of the design are noted where improvements can be made to the reliability or testability, the R&D manager shall be notified for evaluation.

- Design Review 1, 2, 3

  Design reviews shall occur in multiple steps to:

  - Ensure the description of the software to be implemented meets the requirements specifications. The hardware RS/DS and software RS (if required)/DS are inputs to this design review. This refers to the Review 1 block in Figure 17.

  - Ensure the RTL has been properly coded and simulated to proceed to the implementation phase. Also reviewed at this time are the constraint and script files needed for implementation. The updated hardware RS/DS, software RS/DS, RTL (FPGA and Simulation Test Benches), and constraint files are inputs to this design review. This refers to the Review 2 block in Figure 17. Code Analysis is done by a 3rd party tool ALINT-PRO to verify coding syntax and flag potential errors as to assist with Code Review. Code Review is a manual review done by another engineer other than the designer.

  - Ensure the RTL has been properly designed, implemented, and tested to close out the design phase and move into the verification and validation, and integration test phases. This refers to the Review 3 block in Figure 17. This final review shown in the process diagram shall be a comprehensive review of all design activities completed, reports generated, all design documents generated and their released numbers, action item completion status, verifying the storage locations for all files that pertain to the review and design process.

  At each step in the review process, if changes are made to the documents reviewed in previous steps, these changes shall be reviewed as well.

- HDL Coding

  In the next design step, the designer converts the FPGA software design specifications into behavioral descriptions that delineate the functionality required for each module and their interactions. The HDL coding is done by using the information found in the FPGA Design Specification. The coding shall be done in IEEE Std 1364-2001 Verilog HDL. The HDL code is processed by the synthesis tools to generate synthesizable register-transfer level (RTL) representation of the digital logic.

  It is essential that the hierarchy in the behavioral description exactly represents the

design partitioning done during the architectural design step. Any required changes shall be brought to the attention of the author of the FPGA Design Specification for evaluation and approval. If approved, the FPGA Design Specification must be updated to reflect the new architecture.

Verilog HDL language shall be used unless a justification can be made to use VHDL or another HDL language. These must be evaluated by the R&D Development manager in charge of the FPGA development.

Also, the HDL design practices detailed in WI-ENG-103 shall be followed when creating the Verilog modules used in the next step, behavioral simulation.

- HDL Simulation

  The output from the Design Behavioral Coding step (HDL modules) shall be the input to this step. HDL test benches shall be created to thoroughly test each module in the design. Test benches shall be self-checking and scriptable to allow them to be added to a regression test script. Test benches shall be created to apply expected and unexpected inputs to the design under test (DUT). Correct behavior shall be verified for both the expected and unexpected inputs under automated control. Log files shall be generated to note errors that are encountered in running the test benches. These log files shall have a common format in order to provide for automated checking log files during regression testing.

  Example of common format error message
  **** Error => {Module} {Error Message Text} Simulation Time

  Coverage statistics shall be collected. The coverage requirement is 100% statement, branch coverage, expression, and FSM. Justifications shall be created to explain deviations from this requirement and reviewed. Advanced simulation techniques such as constraint-based random stimuli generation, assertion-based verification, and formal verification together with the code coverage analysis should be encouraged for use in the verification of safety-critical FPGA designs as an integral part of the design life cycle. The output of this step is the generation of a behavioral simulation report. The report shall document the simulation results, the storage location of the HDL, test bench(s), and log files. This report is an input to the review which must be held to advance to the logic synthesis step.

- Logic Synthesis and Compilation

  Logic synthesis, in preparation for physical implementation, can be done in multiple steps. The current FPGA device uses two steps, Logic Synthesis using an original equipment manufacturer (OEM) industry standard tool and Logic Compilation, that does optimization, uses a vendor specific tool. Regardless of the number of steps required to generate the files for physical implementation, the Formal Verification tool EC-360 shall be used following each Logic Synthesis step to verify that all RTL specified in the RTL Coding/Simulation step is present prior to in the Physical Implementation step.

- Post-Synthesis/Compilation Equivalency Checking (Formal Verification)

  The Formal Verification tool EC-360 from OneSpin shall be used following the Logic Synthesis Compilation steps to verify that all RTL specified in the RTL Coding/Simulation step is present prior to Physical Implementation step. As explained in the previous section, an alternate path exists to only demonstrate equivalence after the Logic Compilation using the EC-360 tool.

- Physical Implementation (Place/Route Program File Generation)

  Physical Implementation refers to the place-and-route and programming file generation steps in the implementation phase. This can vary from FPGA vendor to vendor, but the end result of the Physical Implementation step is the programming file for the FPGA.

  If place-and-route completes successfully (this is indicated in the report file), then the vendor tool (or approved equivalent) must be used to verify that all register to register delays meet the setup and hold time requirements. When required constraint files can be modified to include false paths, multicycle paths, and paths where approved timing domain crossing is implemented. This part of the place-and-route step is called Static Timing Analysis (STA) or Verify Timing and must generate a report that lists any timing violations. STA shall be done over the required temperature range with worst-case and best-case voltage and process. The report data from this step must be preserved and saved for review after the Test Phase is completed. The vendor supplied tool shall be used to generate the programming file used in the Test Phase for prototype verification.

- Post-Layout Verification (Formal/Timing Verification)

  Performing multiple timing back annotated simulations is an alternative method for completing the post-layout verification step. Multiple simulations shall be done to validate that the FPGA will meet set-up and hold requirements over worst-case and best-case process, voltage, and temperature. In addition, I/O delay specifications from the constraint files shall be verified on all simulations.

- Functional Verification

  At the end of the FPGA Development Process, functional hardware verification shall be performed to confirm correct board/module functionality in the intended operational environment. Functional hardware verification is performed on the entire PCB board with programmed FPGA's using a limited set of input stimuli that covers the input combinations expected during normal operation of the FPGA. Functional hardware verification shall verify that no design issues are present when interacting with the circuitry interfacing with the FPGA device. Items that shall be checked include:
  - Verify that during powerup or programming that no undesirable I/O behavior is observed that will cause any system interaction. Document any I/O behavior

observed and its relationship to onboard devices.
- Verify proper I/O logic levels for external signals.
- Verify appropriate output driving currents are configured and that signal rise/fall times are within interfacing specifications.
- Timing is within specifications for the external devices.
- External clock sources are within device specifications.
- Signal integrity on edge sensitive signals is correct.
- FPGA power voltage levels and ripple are within device specifications, etc.

An additional functional verification step to generate input stimuli that includes input combinations not expected during a normal board operation is performed at the system level to confirm that there are no unexpected responses.

Thermal testing shall be done on the device under test to verify that no functional issues are present in the intended operation range.

5.6 APPLICATION CONTROL

In previous implementations of the HFC-6000 centralized control system, an application program resides in a single remote. The controller reads field inputs from configured AI and DI PCBs via the ICL, executes the application program, and then distributes the resulting outputs to AO and DO PCBs via the ICL. Each I/O PCB manages its end of the ICL communication and its particular I/O channels, but it does no application processing.

For the HFC-FPGA system, each PCB installed in the PCB rack includes a set of I/O channels, and both the HFC-FCPU/HFC-FCPUX modules have the capability of executing application logic. All control functions will reside in the HFC-FCPU/HFC-FCPUX, and the I/O modules will be restricted to controlling their hardware interface with the field equipment. Consequently, the input boards perform input scan and transfer their input data status to the HFC-FCPU/HFC-FCPUX via the F-Link during their mastership period. The HFC-FCPU/HFC-FCPUX executes the application code and if the Control and Diagnostic output data are the same, distributes the updated output data to output modules via the F-Link. The output modules verify received output data, execute signal conditioning, and transfer those data to the output points under their control. The redundant HFC-FCPU/HFC-FCPUX controls regular transfer of application status to the Gateway module via the G-Link, and the Communication Gateway broadcasts the accumulated status to the C-Link during its mastership.

5.7 THE ADOPTION OF HFC-6000 PRODUCT LINE ARCHITECURAL CONCEPTS

The HFC development and change process is strictly controlled and its integration into hardware and software is thoroughly tested. HFC quality assurance programs are applied during the development of the HFC-FPGA system of HFC-6000 platform. HFC-FPGA system adopts hardware and software architectural concepts that are used in HFC-6000 platform as described in HFC-6000 SER as well as HFC TUV SIL 3 certified controller HFC-FPC08. However, when these architectural concepts are adopted, the HFC-FPGA system is treated as new system following disciplined specification and implementation of

design that are required by the HFC QAPM.

The following are some important hardware and software components (or modules) in which their architectural concepts have been adopted for use in the HFC-FPGA system:

- Program algorithms for CQ4 blocks, timers, etc., which are a subset of the total HFC-6000 library modules included as part of the commercial grade dedication process during HFC-6000 SER qualification process, were software components originated as part of the basic features of ECS-1200 developed from 1982 to 1990s. The CQ4 algorithms are migrated into FPGA logic, which are treated as newly developed FPGA firmware.

- The F-Link uses the token-passing protocol developed for the C-Link and backplane hardware traces developed for the ICL. The ICL provides a redundant communication bus between the redundant controllers and I/O modules within the main and extended chassis. The ICL is fully encompassed within the scope of the HFC-6000 platform. The C-Link, designated as the Safety C-Link in HFC-6000 platform, provides a redundant internal network to interconnect platform nodes. The F-Link firmware is treated as newly developed FPGA firmware.

- The G-Link Communication module HFC-FPC08, which provides a gateway communication between the HFC-FPGA controllers and the C-Link, manages communication with the C-Link, and the redundant controller modules control status transfer to the Gateway. This module supports 2 Ethernet ports that are configured to communicate via C-Link with an external Engineering Workstation, and 2 Ethernet ports that support ELPC. The module also supports 2 channels that communicate with a redundant pair of centralized controller modules such as the HFC-FCPU or HFC-FCPUX via G-Link. The earlier version of the HFC-FPC08 was used extensively in the HFC Automatic Seismic Trip System (ASTS) that is currently installed in all South Korean nuclear plants. The G-Link firmware is treated as newly developed firmware.

- All HFC-FPGA I/O cards input/output circuitries are adapted from the HFC-6000 platform I/O cards. All HFC-FPGA I/O cards are treated as newly developed modules.

- The algorithm for HFC-FPUA01, I/O Module for 16 4- to 20-mA AI Channels, was adopted from the corresponding HFC-6000 platform module. The algorithm is used to develop into the new FPGA firmware in the I/O module.

- The algorithms for HFC-FPUL, I/O Module for 8 AI Channels for Type E Thermocouples; HFC-FPUM, I/O Module for 8 AI Channels for 100-Ohm Platinum RTDs; and HFC-FPUM2, I/O Module for 8 AI Channels for 100-Ohm Platinum RTDs were adopted from the corresponding HFC-6000 platform modules. These algorithms are migrated into the FPGA logic, which are treated as new FPGA firmware.

Additionally, the architecture of the One-Step tool for FPGA application was adopted from the early version of the tool that was discussed in the HFC-6000 SER. Similar to its HFC-6000 microprocessor version of the tool, the One-Step used for FPGA applications can create or modify FPGA application program using a development workstation at the HFC facility or an Engineering Workstation (EWS) offline PC workstation in the field. The end programming files created by One-Step are employed to reprogram the FPGAs. To program the FPGA, the programming file is transferred to the FPGA via a serial interface (JTAG) under a secured and documented process while the system is offline.

5.8 HFC CONFIGURATION MANAGEMENT

HFC has established and implemented system configuration management process in accordance with requirements specified in IEEE Std. 828. Configuration Management is used to handle all HFC controls system products and projects. HFC work instruction WI-ENG-003 Configuration Management defines the detail process and methodologies. System configuration management uses the project life cycle model to identify components to be controlled and define the control and change process of the identified components.

The first step is to identify components to be controlled. Components to be controlled are project specific and typically include but not limited to: requirements, design documents, V&V programs and procedures, firmware/application software source codes etc. Each identified SCM component at its final baseline milestone is uniquely identified. It shall include product name, version number, baseline component ID, and date. The ID numbering system that is used for any project or product line applies to formal drawings and internal documents.

Furthermore, HFC has implemented a method of change management to allow for the tracking of changes between revisions of any certified or qualified products. The System Change Request (SCR) Process, as described in WI-ENG-812, is used for changes and updates to HFC products, including by not limited to those covered by a USNRC Safety Evaluation. For any change to a released product covered under the SCR process, the following steps are taken:

1. An SCR is opened by an authorized HFC staff member and is automatically assigned an SCR number.

2. The originator of the SCR provides a projected impact analysis of the change proposed in the SCR and attaches supporting evidence.

3. The SCR is evaluated by the Department Director/Designee, QA manager, and V&V Manager. Each of these reviewers can approve the implementation of the SCR, or request further analysis.

4. Upon the Implementation approval of the SCR by all three reviewers, the initiator of the SCR may begin implementing changes to the hardware/software/system within the scope of the SCR.

5. The changes will be developed and reviewed under the standard HFC design process.

6. Upon completion of the Test Phase for the hardware/software/system, the originator of

the SCR will attach supporting evidence to the SCR to show that all impacted documents and products have been fully tested and the impact of the SCR fully documented.

7. The Department Director/Designee, QA manager, and V&V Manager will review the supporting evidence and either sign off for the closure of the SCR, or request additional information. This supporting evidence will include V&V activities when applicable, such as for products covered by a USNRC Safety Evaluation.

8. The SCR will be closed and retained.

Use of the SCR process ensures that all changes and their impacts are evaluated and recorded such that the information is readily available to stakeholders and regulatory bodies.

6.0 SAFETY SYSTEM DESIGN TOPICS

A nuclear power plant safety system that utilizes the HFC-FPGA system must provide deterministic performance with predictable operation and defined maximum response time characteristics. 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.

This description will define all aspects of deterministic performance including:

- Centralized Controller Module Characteristics,
- I/O Module Characteristics,
- Control/Diagnostic FPGA Characteristics,
- C-Link,
- F-Link,
- G-Link,
- RIF.

6.1 CENTRALIZED CONTROLLER MODULE CHARACTERISTICS

The HFC-FPGA system is configured with a pair of redundant centralized controller modules. Each centralized controller module obtains a station ID based on location in the HFC-BPE01-19 backplane. The controller module with an even address is assigned station address 26 and is referred to as FCPU_A/FCPUX_A. The controller with an odd address is assigned station address 30 and is referred to as FCPU_B/FCPUX_B.

During operation, both controllers are monitoring F-Link data, running application processes, comparing diagnostic data over the HPI, sending application results to I/O cards, and then sending system data to the Gateway Controller via G-Link. If the A controller fails, the I/O data that the B controller generates is used by the I/O modules after a hysteresis period. The centralized controllers utilize a control FPGA and diagnostic FPGA, as described in Figure 18. Figure 18 does not include the onboard I/O present on the HFC-FCPU, as it was not tested within the scope of this amendment.

[

]

Figure 18. HFC-FCPU/HFC-FCPUX Block Diagram

The centralized controllers run application processing for 3.5 seconds, then suspend application processing for a single F-Link cycle. During this suspension of application processing, the application status is sent from the A controller to the B controller via the RIF.

6.2 I/O MODULE CHARACTERISTICS

The HFC-FPGA I/O Modules are independent cards located within the HFC-6000 chassis. Each I/O module has a Control and Diagnostic FPGA, which function as described in Section 6.3. All I/O modules use F-Link to communicate with the controller modules. The I/O modules receive data from controller modules, scan their on-board I/O's, and then transmit the scanned data to the controllers via F-Link.

The I/O module begins initialization on power up, or after the local reset switch is released. After the I/O module is power initialized, the board configuration module reads the setting from RACK/SLOT backplane signals station address. The FPGA global clocks are generated by the clock conditioning circuit using a 25 MHz oscillator as a reference. The F-Link control block verifies the integrity of the Serial Peripheral Interface (SPI) Flash before power up is completed and data transmission on the F-Link can begin. F-Link message validity is determined by a CRC-16 code embedded in the message. Figure 19 shows a generic configuration of the control and diagnostic FPGAs in an I/O module.

[

]

Figure 19. Example HFC-FPGA I/O Module Block Diagram

6.3 CONTROL/DIAGNOSTIC FPGA CHARACTERISTICS

All HFC-FPGA modules utilize a two-FPGA configuration: a Control FPGA and a Diagnostic FPGA. The Control FPGA initiates all HFC-FPGA functionality including communication, application logic processing, and I/O control. The Control FPGA also monitors the diagnostic FPGA for any errors, and may reset the Diagnostic FPGA if errors are detected.

The Diagnostic FPGA receives the same input data as the Control FPGA. The Diagnostic FPGA validates the process step performed by the Control FPGA. Quality information generated by I/O modules and diagnostic processing is used to dictate application process action or inaction. Error reporting from important system resources is also processed and used to create diagnostic status information for transmission with the F-link payload. A high-level summary of diagnostic functions is:

- F-link Engine
    - Maintains CRC validation of transmit and receive payloads.
    - Uses CRC validation and the existence of a receive payload to determine the operational status of other FPUs in the system.
    - Maintains CRC validation of internal memory components at run time.
    - Reports diagnostic and/or error information to the diagnostic processing module.
    - Controls physical link enable logic while monitoring outgoing payloads.
- F-link Filter

  - Assigns quality information to incoming data based on payload status received from the F-link engine.
  - Maintains CRC validation of the filter flash memory prior to use.
  - Maintains CRC validation of internal memory components at run time.
  - Reports diagnostic and/or error information to the diagnostic processing module.
- Application Processing Module
  - Assigns quality information to processed data based on application process results.
  - Maintains CRC validation of internal memory components at run time.
  - Reports diagnostic and/or error information to the diagnostic processing module.
- I/O Pre/Post Process Module
  - Assigns quality information to processed data based on I/O channel health status.
  - Maintains CRC validation of internal memory components at run time.
  - Reports diagnostic and/or error information to the diagnostic processing module.

6.4 C-LINK

The redundant C-Link communication is utilized in the same manner in the HFC-FPGA system as described in the approved HFC-6000 system. The C-Link communication design utilizes a token passing protocol for deterministic communication with other safety systems within its own division.

The C-Link processor initializes on power up or reset, and hardware and software associated with the C-Link processor are validated by diagnostics during initialization. The C-Link processor also sets up its Private and Public Memory during initialization. The communication ports remain disabled during initialization becoming enabled when real-time operation is initiated by the gateway HFC-FPC08.

In the redundant gateway configuration, the C-Link processor on the primary gateway HFC-FPC08 performs all broadcast operations. The secondary processor listens to all broadcast messages and stores the data in public memory on the gateway. No further processing is performed on the data unless it becomes the primary gateway.

The C-Link processor performs diagnostics that include validation of the C-Link hardware and software, CRC-32 checking to validate messages, and logging any communication errors on the C-Link. It includes network connectivity and communication status of each node. The status of the diagnostics is copied to Public Memory and is used by the SYS processor in determination of overall system status. The safety function will not be inhibited nor be deadlocked by outside equipment due to the communication architecture of the safety C-Link.

C-Link is only used in the Gateway HFC-FPC08, and is not present on the HFC-FPGA I/O or control modules.

6.5 F-LINK

The F-Link communication protocol is used to allow I/O modules and controllers in the HFC-FPGA system to communicate with each other. The F-Link structure is based on the ICL token-passing protocol concept used in the HFC-6000 microprocessor-based platform. The F-Link FPGA software within each HFC-FPGA module accesses external F-Link traces via redundant RS-485 transceivers on each module. Each module within the chassis is assigned a station address based on backplane location. The modules then communicate using a similar token-passing protocol and message packet structure to that used by C-Link and detailed in Section 5.1.4. Table 4 shows the similarities and differences between the C-Link, F-Link, and G-Link token-passing protocol.

Table 4. Token-Passing Protocol Comparison

Description	F-Link	G-Link	C-Link
[			
			]

Description	F-Link	G-Link	C-Link
[			
			]

The F-Link protocol is designed such that only data that matches the F-Link packet structure will be transmitted or received. Any packet deviating from this structure is rejected and the system is notified via an error counter.

The token-passing structure for the F-Link functions is described in Figure 20.

[

]

Figure 20. State Diagram for Token-passing Mechanism

6.6 G-LINK

The G-Link communication protocol is used to pass information from the HFC-FPGA centralized controllers to the HFC-FPC08 Gateway controllers. The G-Link functions in the same manner as the F-Link with respect to overall architecture and rejection of incorrect data. The differences between the C-Link, F-Link and G-Link are detailed in Table 4. Token-Passing Protocol Comparison.

The G-Link allows for communication between the HFC-FPGA system and the EWS, and therefore loss of G-Link function will not impact the ability of the system to perform safety functions.

6.7 DETERMINISTIC PERFORMANCE CONCLUSION

The HFC-FPGA system is designed to have deterministic performance with predetermined maximum response time for changing input signals, and communication with external equipment. This is accomplished by the deterministic behavior of the F-Link cycle utilizing a 6.8 ms fixed cycle time and packet structure as detailed in Table 4. Information is provided to output modules from the centralized controller via the same F-Link communication. Memory update in the controller is only updated before running of the application processing. The duration of application processing is variable as the user defines how many analog (CQ4) blocks are included, but is a deterministic duration for a defined application.

For each individual HFC-FPGA module, an FMEA was performed encompassing the failure modes of all major active components. The components used in each HFC-FPGA module were evaluated for failure rate, failure mode, possible causes of failure,

symptomatic effects, method of detection, effects on the module and system, and method of remediation for a given failure. The results of this FMEA show that all major potential hardware failures have a known and deterministic method of failure, each of which is detectable by the HFC-FPGA system and can be communicated to the user. Details of the FMEA results are given in RR901-107-01.

6.8 QUALITY ASSURANCE PROGRAM

The HFC Quality Program used for the development of the HFC-FPGA system is an updated version of the Quality Program used for the development of the HFC-6000 system from the original qualification submittal. This updated program is designed to comply with NQA-1b-2011 Addenda to ASME NQA-1-2008, NQA-1-2012, and NQA-1-2015, "Quality Assurance Requirements for Nuclear Facility Applications," including the exceptions and clarifications identified in USNRC RG 1.28 Revision 5, Section C. In following these industrial standards and regulatory guidance, the HFC Quality Assurance Program complies with 10 CFR 50 Appendix B; "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants", and 10 CFR Part 21. The HFC Quality Assurance Program also complies with ISO 9001.

The HFC software quality assurance plans follow the guidance of IEEE Std 730-1989, "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 lifecycle were patterned after those described in BTP 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems". HFC-FPGA Verification and Validation efforts follow those described by IEEE Std 1012, "IEEE Standard for System and Software and Verification and Validation".

The QA program includes procedures for managing the multidisciplinary interfaces within the HFC design effort and clearly delineates the responsibilities for quality functions in the respective organizations. To assure that the documentation reflects current design, the QA Program, includes procedures and methods that ensured the correctness and completeness of the documentation at the end of each phase of the HFC-FPGA design project. The ultimate objective was to eliminate all design errors as early as possible and ensure that the design basis, safety, operational and maintenance requirements were properly considered. This ensured that the resulting HFC-FPGA product met the highest standards of technical quality.

The HFC QAPM is organized such that sections 1 to 18 correspond directly with sections 1 to 18 of 10 CFR Part 50 Appendix B. Each section of the QAPM lists associated QPP documents within the HFC Quality Program that details methods and instructions on how to carry out quality-related activities. The sections of the QAPM are as follows:

1. Organization
2. Quality Assurance Program
3. Design Control
4. Procurement Document Control

5. Instructions, Procedures, and Drawings
6. Document Control
7. Control of Purchased Items and Services
8. Identification and Control of Items
9. Control of Processes
10. Inspection
11. Test Control
12. Control of Measuring and Test Equipment
13. Handling, Shipping, Storage and Preservation of Items
14. Inspection, Test and Operating Status
15. Control of Nonconforming Items
16. Corrective Action
17. Quality Assurance Records
18. Audits
19. Contract Review
20. Servicing and Customer Supplied Products
21. Statistical Techniques

To assure that the HFC QA Program rigorously adheres to the Programs mandated, periodic 3rd party independent verification assessments are conducted to assure compliance with the QA Program. Furthermore, this verification provides ongoing assessment of the adequacy of the measures undertaken to ensure technical correctness of the QA processes.

The HFC QA program continuously revises quality procedures, policies, and to ensure compliance with the most recently endorsed versions of quality standards and regulations.

Software quality was verified per the guidance of IEEE Std 7-4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations" which incorporates guidance from ASME NQA-1a Part 2.7 as part of the document release process.

6.9 REGULATIONS, CODES, STANDARDS AND GUIDANCE FOR DIGITAL SYSTEM IMPLEMENTATION

6.9.1 General

Listed below are the regulatory documents, codes, standards, and regulatory commitments that are applicable to the design, implementation, and maintenance of the HFC-FPGA system addressed in this amendment.

6.9.2 Compliance with USNRC Documents

DI&C-ISG-04 "Highly-Integrated Control Rooms—Communications Issues", Rev. 1, 2009

The HFC-FPGA platform utilizes the C-Link for all external communication including communication with non-safety entities. This includes all operator workstations and displays. The F-Link and G-Link communication used by the HFC-FPGA platform does

not interface with any equipment or modules outside of its own division. The HFC-HSIM modules is used to facilitate F-Link communication between channels within the same division. With respect to the NRC Staff Positions in Section 1 on Interdivisional Communication, the HFC-FPGA platform adheres to DI&C-ISG-04 as follows:

1. The C-Link provides intra-divisional communication capability for communications between safety related controllers and non-safety related equipment. The C-Link intra-divisional communication capabilities are unidirectional to non-safety related equipment, broadcasting data from the HFC-FPC08 gateway Module to the non-safety EWS.

2. The C-link does not communicate with any outside division. The only non-divisional communication capability of the C-Link is the transmittal of information/data to non-safety related equipment. This transmission only has a one-way capability through fiber optic cabling due to the design of the HFC-FPC08 gateway. The safety related function can only transmit to the non-safety related equipment and not vice versa. The HFC-FPGA platform does not have inputs from other divisions that can inhibit or delay the safety function of the division in question. HFC-FPGA operation is sustained given a malfunction, design error, communication error or software error/corruption outside of its division

3. The C-Link does not communicate to other safety divisions. The F-Link provides communication to only controllers within its own safety division via the HFC-HSIM module, and does not connect the F-Link to anything outside its own safety division. The communication path available on the C-Link to non-safety related equipment is only one-way to the non-safety related equipment through an HFC-FPC08 gateway. This prevents the non-safety related equipment from affecting the safety related equipment. The specific safety functions performed by the HFC-FPGA system will be evaluated on a plant-specific basis.

4. The HFC-FPGA platform utilizes separate modules for external communication and execution of safety functions. In the event of a failure on the HFC-FPC08 gateway, the safety function execution on the HFC-FCPU/FCPUX controller module will not be affected. Section 5.6 details the application control of the HFC-FPGA platform.

5. Cycle time for each I/O scan is set by the 6.8 ms F-Link cycle. Each safety application will have a set cycle time dependent on the specific application. The deterministic nature of application cycle times is detailed in Section 6.7.

6. The safety function processor does not perform handshaking and does not accept interrupts from outside its own safety division. The HFC-FPGA platform does not communicate with equipment outside of own division with the exception of communication to non-safety related equipment via C-Link.

7. A predefined data set, the Dynamic Database (DDB), defined by Request Tables (RQ) is used by the HFC-FPGA system. An RQ Table includes the information that identifies which data points to include in the broadcast. Message structure for all

data on all links is strictly defined as detailed in Table 4, and any data not meeting this structure will be rejected and error flags will be set.

8. HFC has ensured that the designs of the C-Link capabilities are such that a division does not exchange information/data between other safety divisions. The broadcast over the C-Link from a safety related channel/division to the non-safety related equipment is one-way through the HFC-FPC08 gateway. Therefore, the non-safety related equipment does not affect the safety function in any manner

9. The C-Link software is based on a network layer structure. Each message received is passed from a lower layer to the next higher layer and interpreted by each layer in sequence. The message data is transferred from the Ring Buffer in the NIC shared memory to local private memory, and then to the Public Memory where the communicated information is stored in designated memory locations. These memory locations are not used for any other purpose. Each message to be transmitted is passed from a higher layer to the next lower layer and processed by each layer in sequence. The message data is transferred from Public Memory to local private memory, and then to the Ring Buffer in the NIC shared memory where incoming and outgoing messages are segregated in separate memory locations. Input and output data are always stored in separate predetermined memory locations in Public Memory. The C-Link controller extracts the required data from the incoming buffer and copies the valid message data to the allocated receiving database in Public Memory. The segregation of the transmitted database and received database are predefined through BLRQ tables. This method provides acceptable segregation of input and output data.

10. Application alterations can only be performed when the HFC-FPGA System is offline. The Control and Diagnostic FPGA can only be reprogrammed by removing the HFC-FCPU/FCPUX controller module from its installation location and using a specialized connector. The specialized connector can be used to link a programming workstation with the appropriate installed programs to the HFC-FPCU/FCPUX. The programming workstation cannot physically be connected to the HFC-FPGA system during normal operation. It is not possible to reprogram any FPGA module in the HFC-FPGA system using the C-Link connected non-safety EWS.

11. C-Link communication does not have the capability to alter any software or firmware on the controller processor or on the communication processors. The only information being communicated deals with information or data from the public memory and software instructions are not capable of being transmitted. Interdivisional communication is not allowed and is not part of the HFC-FPGA architecture.

12. Required safety functions executed by the HFC-FPGA system are unaffected by faults originating in non-safety equipment, by way of a three-level defensive design. Firstly, the HFC-FPC08 gateway does not receive messages from non-safety equipment, as it is only able to broadcast data out of the system to non-safety equipment. Secondly, The C-Link processor has redundant communication

channels with a separate NIC for each channel. Because the termination of transmission can occur at different times on the two channels, synchronization between the two channels is necessary for transmitting and receiving data in order to use the token passing protocol. The design of the C-Link Protocol contains the messages verification scheme and synchronization rules to eliminate the corrupted messages. Thirdly, the HFC-FCPU/FCPUX controller modules compare the G-Link data arriving form the redundant HFC-FPC08 gateway modules and will reject the data with an error flag if the messages do not match the pre-defined message structure, or each other.

13. All communications of the HFC-FPGA system that are used for voting purposes undergo CRC checking as described in Section 6.3, as well as error detection via the Diagnostic FPGA as described in Section 5.3.2. In the event of a single error in the primary controller, the HFC-FPGA system will set the primary HFC-FPCU/FCPUX controller to a failed state and fail over to using the data from the secondary HFC-FCPU/FCPUX. This ensures that any communications vital to the safety function of the system are maintained. Specific safety functions will be evaluated on a plant-specific basis.

14. All vital communication for the HFC-FPGA system is performed using point-to-point methods. The C-Link communicates over a redundant fiber optic cable as the dedicated medium. F-Link and G-Link communication is performed over dedicated backplane traces. All messages are passed directly from the sending node to the receiving node without the involvement of equipment outside the division of the receiving or sending node.

15. The F-Link communication operates on a fixed 6.8 ms cycle, sending and receiving data between I/O modules and the controller modules. The details of F-Link packets are show in Table 4. The F-Link cycle interval and what data is transmitted on the F-Link is independent of any state changes in data. The specific I/O points and associated data sent and received will be evaluated on a plant-specific basis.

16. The HFC-FPGA system is designed to perform its safety function without any communication with non-safety related equipment or other safety divisions. The C-Link only connects to the non-safety EWS to send information as a one-way communication path. This connection will not cause the safety functions of the HFC-FPGA system to stall, deadlock, or livelock. This functionality will be verified on a plant-specific basis.

17. The heat and EMI/RFI conditions discussed in Section 8.2 were used as a generic qualification environment for the HFC-FPGA system. Communication pathways such as optical fibers and the communication backplane were included in the VV0115 Qualification Test Specimen, as detailed in Table 6.

18. Hazard analysis for the HFC-FPGA system including communication protocols was performed as part of the V&V analysis associated with each phase of platform design.

19. The C-Link, F-Link and G-Link are all token-passing communication protocols, in which token passing occurs in a defined sequence. The token-passing sequence continues from module to module in a continuous loop that permits each module to transmit its data in a repetitive cycle to provide a fixed response time. When the module is not holding the token, it is listening to the other module broadcasts and determining which messages contain data that it needs to receive.

    By design, it has been determined that all links and nodes have the capability to handle the maximum error rate calculated for a system. The Token passing design prevents excessive communication of data over each link. The true data rate is identified for each plant specific application. This includes the design overhead, which ensures that communication bandwidth is sufficient to ensure proper performance of all safety functions. Communications throughput thresholds and safety system sensitivity to communications throughput issues will be confirmed by testing on a plant-specific basis

20. Response times have been evaluated for a generic safety application as discussed in Section 8.2.2. This item will be reviewed on a plant specific basis as well.

With respect to the NRC Staff Positions in Section 2 on Command Prioritization, the HFC-FPGA platform does not function as a "Priority Module". Use of the HFC-FPGA platform for priority module functionality can be evaluated on a plant-specific basis.

With respect to the NRC Staff Positions in Section 3 on Multidivisional Control and Display Stations, all Engineering Workstations (EWS) used with the HFC-FPGA platform within the scope of this amendment are non-safety display stations. The HFC-FPGA platform adheres to DI&C-ISG-04 as follows:

1. All non-safety EWS are connected via one-way communication to receive data from the HFC-FPGA system via C-Link. There is no data sent from the non-safety EWS to the HFC-FPGA system. The non-safety EWS does not control operation of safety-related equipment. Any loss of function or malfunctions of the non-safety EWS will not impact the execution of safety functions of the HFC-FPGA system.

2. The use of safety-related controls and displays with the HFC-FPGA system will be evaluated on a plant-specific basis

3. A D3 analysis will be performed on the plant-specific application of the HFC-FPGA system.

DI&C-ISG-06 "Licensing Process", Rev. 2, 2018

The HFC-FPGA platform complies with the guidance set forth in DI&C-ISG-06, as a Tier 1 amendment to the PP901-000-01 HFC-6000 Topical Report. In-depth details of compliance with this ISG are listed in VV901-115-09, NRC DI&C ISG-06 Requirements Compliance Traceability Matrix for HFC-FPGA Controller. On a more general level, the HFC-FPGA system architecture is detailed in Section 5.0, equipment qualification is detailed in Section 8.0, the development process is detailed in Sections 5.2 and 5.4, and the

SDOE is detailed in Section 6.11.2 of this report. Compliance with IEEE Std 603 and IEEE Std 7-.43.2 is detailed in Section 6.9.3 of this report. For areas of this ISG that require application-specific analysis, compliance will be analyzed on a plant-specific bases.

RG 1.22 1972 "Periodic Testing of Protection System Actuation Functions"

The HFC-FPGA platform conforms to this Regulatory Guide (RG). Design principles have been employed that facilitate periodic testing of the HFC-FPGA system to verify its ability to perform protective initiation functions. The HFC-FPGA system allows complete testing of its actuated devices in accordance with the RG. The C-Link communication between the HFC-FPGA gateway module and external Engineering Workstation is configured to be one-directional during normal plant operation. It is possible to provide the capability for sending DDB data to the HFC-FPGA gateway using a specialized EWS configuration, allowing for the routine testing of actuated equipment during plant shutdowns. The testability of protection systems will be evaluated on a plant-specific basis.

RG 1.28 2017 "Quality Assurance Program Criteria"

The HFC-FPGA system is developed and maintained under HFC's Quality Assurance program, as outlined in the HFC Quality Assurance Program Manual. This includes the retention of records for nuclear projects, audit frequency and content, and the documentation process for quality issues. HFC's Quality Assurance Program is designed to comply with NQA-1b-2011 Addenda to ASME NQA-1-2008, NQA-1-2012, and NQA-1-2015, "Quality Assurance Requirements for Nuclear Facility Applications," including the exceptions and clarifications identified in USNRC RG 1.28 Revision 5, Section C. By following these industrial standards and regulatory guidance, the HFC Quality Assurance Program complies with 10 CFR 50 Appendix B. The HFC Quality Assurance Plan undergoes periodic audits to ensure that execution of the Quality Assurance Plan meets the documented requirements. Details of the HFC QA program are shown in Section 6.8.

RG 1.47 2010 "Bypassed and Inoperable Status Indications for Nuclear Power Plant Systems"

HFC-FPGA modules include a run switch, which allows for the ability to disable the function of each module individually. Each module also has LED indication of status, and sends notification of inoperable status to the EWS. Specific bypass and status indication requirements will be evaluated on a plant-specific basis.

RG 1.53 2003 "Application of the Single-Failure Criterion to Nuclear Power Plant Safety Systems"

The HFC-FPGA system is designed to detect, report, and perform deterministically in the event of single failures. The system architecture is structured such that the failure of any single module will be detected and reported to the EWS as an alarm. The failure of any single module will not cause the failure of any other module. For I/O modules, this is done by using the token-passing F-Link protocol. For gateway and controller modules, each remote in the HFC-FPGA system is configured with redundant controllers and gateways. At the hardware level, an in-depth analysis of the failure modes and effects has been

performed for each HFC-FPGA module to ensure that all hardware failures are detectable and are reported at the system level. On the FPGA level, all HFC-FPGA modules utilize a diagnostic FPGA to detect any single failures within the control FPGA, including SEUs. Any failures at the FPGA level are reported at the system level. Design analysis for the effects of single failures was performed per IEEE Std 379-2000. The report RR901-107-01, "FMEA for the FPGA Controllers of HFC-6000 Safety Platform" contains the component-level details of the results of this analysis.

Evaluation of design basis events and common cause failure from a single-failure event will be evaluated on a plant-specific basis.

RG 1.62 2010 "Manual Initiation of Protective Actions"

The HFC-FPGA system can be configured for manual initiation, using I/O modules. This functionality can be enabled or disabled dependent on system configuration. Plant-specific evaluations shall be made of the system to verify this functionality at a system level.

RG 1.75 2005 "Independence of Electrical Safety Systems"

The design of the original HFC-6000 system addressed in PP901-000-01 conforms to this RG, and the HFC-FPGA uses the same power distribution hardware as the original HFC-6000 system. The field-implementation of the HFC-FPGA (e.g., the connecting wires, cables, switches and relays) will also conform to the physical, mechanical and electrical separation standards provided by the guide as well as IEEE Std 384. A plant-specific implementation will provide further details regarding physical independence. The HFC-FPGA modules addressed in this amendment are designed to function in an identical configuration with respect to electrical systems as the qualified HFC-6000 system.

RG 1.100 2009 "Seismic Qualification of Electrical and Mechanical Equipment for Nuclear Power Plants"

The HFC-FPGA 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 number of Operating Basis Event (OBE) and Safety Shutdown Event (SSE) seismic stress tests, at levels specified in EPRI TR-107330. The seismic spectra from EPRI TR-107330 are used as a generic set of harsh conditions for qualification purposes per the guidance in IEEE Std 344-2004, and site-specific seismic requirements will be addressed on a site-specific basis using experience data from the installation site. Details of generic seismic qualification are discussed in detail in Section 8.2.4.5.

RG 1.105 1999 "Setpoints for Safety-Related Instrumentation"

HFC-FPGA modules were measured to be within the accuracy acceptance criteria listed in Section 8.2.2 before, during, and after all qualification testing as part of operability testing to ensure that modules will be able to send and receive setpoint data accurately. Set points will be evaluated on a plant-specific basis.

RG 1.118 1995 "Periodic Testing of Electric Power and Protection Systems"

The HFC-FPGA modules include the logic detection for open and out of range AI/AO channels built into system hardware and firmware for direct verification of field equipment. Verification of logic states is achievable using the EWS, such that the HFC-FPGA system can support periodic testing. Additional utilities for periodic testing will be implemented and evaluated as part of a specific application on a project-by-project basis.

RG 1.152 2011 "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"

The qualified computers and tools for use with the HFC-FPGA system are similar in function and design methodology to those developed for the qualified HFC-6000 system and modules. The software running on the Engineering Workstation used as a communication device external to the HFC-FPGA is segregated into both pre-developed and new (application) software. For the new safety related software running on the EWS, HFC has implemented methods employed for designing, verifying, validating and implementing software to be used in safety related systems that follow the HFC software quality plan, and are consistent with this RG, IEEE Std 7-4.3.2, and ASME NQA-1. This development, testing, and qualification plan addresses all of the runtime resident computer software on the Engineering Workstation. Specifics of software qualification for the HFC-FPGA system are covered in Section 7.0.

The design process for the HFC-FPGA system utilizes several layers of protection against undocumented, unwanted, and unneeded modifications. The development and operational environment for the HFC-FPGA system has undergone a vulnerability analysis as detailed in Section 6.11.1. Potential vulnerabilities have been mitigated by strategies and the implementation of a SDOE, as detailed in Section 6.11.2.

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-FPGA modules. Details regarding compliance with IEEE Std 603 are discussed in Section 6.9.3 of this document.

RG 1.168 2013 "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 lifecycle as provided in BTP7-14 and IEEE Std 1012-2004. Lifecycle phases for plant operation will be provided during plant-specific implementation. HFC has documented an acceptable software development methodology and follows this methodology consistently in developing any safety-related new software, including that for the HFC-FPGA system. This program is comparable to that used for software in the qualified HFC-6000 system and modules with additional FPGA-specific V&V tasks added to the implementation and validation phases. The additional tasks included Timing Simulation, Static Timing Analysis, Module Fault Insertion Testing, Logic Equivalency Verification, and Post-Layout Simulation, as detailed in Sections 5.4 and 5.5. Anomaly reporting within V&V process for the HFC-FPGA

system was performed per IEEE Std 1012-2004.

RG 1.169 2013 "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-FPGA system's software. This plan was formulated based upon the guidance provided by IEEE Std 828 and IEEE Std 1042 for the qualification of the HFC-6000 system, and has been used for the development and maintenance of the HFC-FPGA modules. For each HFC-FPGA module, the FPGA code is evaluated for version management and the overall FPGA load. This evaluation includes checked in code in HFC's Version Manager Tool, SourceSafe, BOM revisions, and source code comments. The evaluation of compliance with HFC's SCM Plan was performed for each phase of development, and a corresponding SCM report was generated and updated for these phases. All changes to released FPGA code utilized complete and detailed System Change Requests to justify the change, along with the associated documentation for design change, testing, and release as detailed in Section 5.8. HFC's SCM is designed to be extended to plant-specific applications.

RG 1.170 2013 "Software Test Documentation for Digital Computer Software Used In Safety Systems of Nuclear Power Plants"

The HFC-FPGA software test plan includes the following items:

- Items to be tested,
- Required features of the modules under test,
- Overall test strategy and approach,
- Detailed description of the test environment,
- Information on the test group and staff,
- Test sequence,
- Test equipment/tools and calibration information,
- Acceptance criteria, and
- Reports containing input listing, output list, test data, error logs, and conformance to acceptance criteria.

For all HFC-FPGA modules, test plans, test specifications, and test reports are generated in accordance with IEEE 829-2008, by incorporating all items required for IL4 documentation into HFC's document structure. All HFC-FPGA modules are treated as IL4 for all phases of development. All traceability and document retention for software testing follows the IEEE 829-2008 guidance for IL4 items.

RG 1.171 2013 "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"

The software testing conducted in the course of HFC-FPGA development has been written to follow both the guidance contained in this RG and in the endorsed IEEE Std 829-2008 and IEEE Std 1008-1987. HFC has developed its software test plans and procedures to address the criteria and guidance of Section C of the RG. Particular emphasis was given to

ensure that the test plans and procedures address the items listed in Section C.1 a-h. The test plans and procedures were generated to cover specific requirements listed in the SRS for software modules, and test plans and procedures were generated by both the engineering development team and the independent V&V team. Test plans and procedures for the HFC-FPGA modules were developed under the same program as those in the initial HFC-6000 qualification addressed in PP901-000-01, with updates to the relevant QPP and WI documents to address updates in regulatory stances. Details of the updated design process are given in Section 5.4 and 5.5. The specific test steps taken for digital computer software used in the EWS that communicates with the HFC-FPGA system are detailed in Section 7.0.

RG 1.172 2013 "Software Requirements Specifications for Digital Computer Software and Complex Electronics Used in Safety Systems of Nuclear Power Plants"

Software requirements specifications for the HFC-FPGA system were written to comply with and reviewed against the guidance in this RG, as well as the associated sections of IEEE Std 830-1998 and IEEE Std 1074-2006. These requirement specifications were written and evaluated as described in Section 5.4 and 5.5 to ensure that all requirements are correct, complete, consistent, testable, traceable, and verifiable. All changes to requirement specifications are evaluated to determine any impact on other phases in the design process as part of the Configuration Management Analysis and Requirements Traceability Analysis of each phase. Process applications are reviewed on a plant-specific basis.

RG 1.173 2013 "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 1074-2006 provide a structured approach for the development of a software lifecycle program consistent with regulatory guidance. This software lifecycle program was used for the original HFC-6000 qualification, and continued for the development of HFC-FPGA modules. All HFC-FPGA modules are classified as new products with the integrity level IL4 and follow the lifecycle process detailed in Section 5.4. This includes V&V Software Safety Analyses performed per IEEE 1012-2004 for the Requirements, Design, Implementation, and Test phases. The complete HFC-FPGA development process meets the intent of IEEE 1074-2006 and BTP 7-14 by following the guidance of IEEE 1012-2004.

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

The HFC-FPGA modules were tested per the requirements of this RG as detailed in Sections 8.2.4.2, 8.2.4.3, and 8.2.4.4.

RG 1.209 2013 "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear

Power Plants"

Environmental qualification details and results for HFC-FPGA modules are given in Section 8.2.4.1. The harsh environmental conditions from EPRI TR-107330 Figure 4-4 were used for generic platform qualification in place of plant-specific harsh environmental conditions.

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

A discussion of its generic concept for meeting Diversity and Defense-in-Depth guidelines as provided in BTP 7-19 is given in Section 6.10 of this report. Details regarding this concept will be provided during plant-specific implementations.

NUREG-0800 "Standard Review Plan (SRP Chapter 7)"

The design of the original HFC-6000 qualification system follows the guidance presented in Chapter 7 of this NUREG. The HFC-FPGA modules were designed to follow the same guidance, as described below.

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

The HFC-FPGA system design as presented does not employ isolation devices with the exception of the C-Link communication to non-safety-related equipment. The electrical isolation for this is through fiber optic cabling and the data isolation is a one-way directional gateway. There are no other interfaces to other systems outside of its division as this is a single channel presentation. For plant-specific applications, isolation devices used in conjunction with the HFC-FPGA will be qualified in accordance with this BTP. This is a plant-specific review item.

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

The HFC-FPGA module software development lifecycle considers the guidance provided with this BTP. The HFC-FPGA new safety-related software was developed using software development plans that detail tasks to be performed from the Requirements Phase through the Validation Phase. The Validation Phase from this BTP is equivalent to the Test Phase in HFC documentation. For each HFC-FPGA module and the platform as a whole, the following items were performed and documented:

- Safety Analyses,
- Verification and Validation Analysis and Testing,
- Configuration Management,
- Testing Activities.

Management, implementation and resource planning procedures were established for new software, in the following areas:

- Software Management Plans,
- Software Development Plans,
- Software Quality Assurance Plans,
- Software Integration Plans,
- Software Safety Plans,
- Software V&V Plans,
- Software Configuration Management Plans,
- Software Test Plans.

The functional characteristics and software development characteristics noted in the BTP were established and met by the HFC process. Details of the development process are discussed in Section 5.4 and Section 7.0. Tasks in the installation, operation, and maintenance phases will be addressed on a plant-specific basis.

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

The HFC-FPGA modules are designed for in-service testability of FPGA hardware and software components. Failure Mode Effects Analysis was performed for each HFC-FPGA module listed in Table 1 and is detailed in RR901-107-01. All major active components used in each HFC-FPGA module were evaluated for failure rate, failure mode, possible causes of failure, symptomatic effects, method of detection, effects on the module and system, and method of remediation for a given failure. For failure modes which were detected using self-test features, these self-test features were tested during hardware/software integration testing in the Implementation phase. Self-testing and failure mode analysis at the system level will be evaluated on a plant specific basis.

NUREG-0800 BTP 7-18 "Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems"

The HFC-FPGA system has been designed to address the applicable sections of GDC 21, as well as RG 1.152 and IEEE Std 7-4.3.2. Tools, and peripheral components were tested and evaluated to a level commensurate with the system they are designed to support, as discussed in Section 7.0. All changes to these items are controlled under the configuration management system described in the QAPM and Section 5.8. Specific applications are viewed on a plant-specific basis.

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 6.10. 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"

The HFC-FPGA modules were designed to meet the timing requirements detailed in EPRI TR-107330. These timing requirements were used for a generic set of acceptance criteria

to evaluate the system performance during qualification testing and are detailed in Section 8.2. Additionally, the system-level communication links were evaluated for deterministic performance, as detailed in Section 6.7.The system-level configuration for plant-specific implementation may impose further requirements to be evaluated on a plant-specific basis.

BTP 7-1 through 7-10, 7-12, 7-13, SRM to SECY 93.087 II.Q, 93.087 II.T

Compliance with these requirements will be assessed on a plant-specific basis.

6.9.3 Compliance with 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-FPGA modules were developed using the same overall design program as the original HFC-6000 system, with FPGA-specific tasks added to the Implementation and Test phases of development. These additional FPGA-specific tasks are described in Section 5.2 for hardware development and Section 5.4 for FPGA development.

All software used in the HFC-FPGA system was developed under HFC's QA Program as detailed in Section 6.8. This QA program is designed to fulfill the quality assurance requirements put forth in NQA-1b-2011 Addenda to ASME NQA-1-2008, NQA-1-2012, and NQA-1-2015, "Quality Assurance Requirements for Nuclear Facility Applications," including the exceptions and clarifications identified in USNRC RG 1.28 Revision 5, Section C. The HFC QA Program is designed to closely conform to 10 CFR 50 Appendix B, as detailed in the Section 6.8 and the HFC QAPM.

HFC-FPGA system is specifically developed for nuclear applications and therefore is not considered commercial grade digital equipment. The vendor-specific IP cores used in the HFC-FPGA system as discussed in Section 5.3 have been evaluated as part of the design process of the FPGA load. For this reason, Clause 5.4.2 of this standard is not applicable to the review of the HFC-FPGA platform.

Software qualification was performed in environments that are representative of those used in installed HFC-FPGA systems, for all software, control FPGAs, and diagnostic FPGAs. This includes exercising and monitoring memory, processors, inputs and outputs, diagnostics, associated components, communication paths, and interfaces. The TSAP developed for the VV0115 Qualification Test Specimen was used as a generic platform example of safety features to be executed. Operability and Prudency testing as described in Section 8.2 demonstrated that the performance requirements related to safety functions were met. These safety features included exercising and monitoring memory, FPGA status, timing, input and output functionality, diagnostic FPGA function, communication paths, and interfaces. Application software will be evaluated on a plant-specific basis.

IEEE Std 279-1971 "Criteria for Protection Systems for Nuclear Power Generating Stations"

The HFC-FPGA system and module-level requirements were generated to be in compliance with IEEE Std 279. The VV0115 Qualification Test Specimen was designed to as a generic safety system capable of providing the protection functions specified in IEEE Std 279-1971. The harsh environmental conditions detailed in Section 8.2 simulate a generic range of conditions under which the HFC-FPGA system is designed to operate. The system has a structure of F-Link communication, redundant controller modules and gateway modules such that the failure of any single module will not result in the failure of the system as a whole. All modules in the HFC-FPGA system follow the QA process detailed in Section 6.8 and have undergone equipment qualification per Section 8. The system is connected to an Engineering Workstation to allow for testing and calibration in general, as demonstrated by the system qualification tests detailed in Section 8.2. Connection with the EWS allows of on-line information read-out of point values, logic values, and alarm statuses. Each HFC-FPGA module has a unique serial number identifier, as well as a module-level part number as listed in Table 1 to facilitate system repair when required.

Channel independence, system interaction, system inputs, and sensor checks will be evaluated on a plant-specific basis. Specific test cases, calibration, bypass capability, specific protective actions, manual initiation, and specific protective actions will also be evaluated on a plant-specific basis.

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

The HFC-FPGA modules were tested and qualified under the harsh environment conditions detailed in Section 8.1. The qualification conditions provided in EPRI TR-107330 Figure 4-4 were used as a generic set of harsh environment conditions. The Qualification Test Specimen for the HFC-FPGA system is a generic platform, so no plant-specific environmental data was available for the scope of this amendment. Additional qualification testing will be performed as needed on a plant-specific basis.

IEEE Std 344-2004 Revised "IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations"

The HFC-FPGA modules were qualified per the seismic qualification criteria in this standard, as detailed in Section 8.1.4.3.3 and 8.2.4.5. The Qualification Test Specimen for the HFC-FPGA system is a generic platform, so no plant-specific seismic data was available for the scope of this amendment. The seismic spectrum from EPRI TR-107330 Figure 4-5 was used as a generic qualification envelope. Additional seismic testing will be performed as needed on a plant-specific basis.

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

The reliability analysis for the HFC-FPGA modules was performed using the PTC Windchill program, referred to at times by the name "Relex 2011". The analysis was

performed using guidance from this IEEE Std, and the mathematical models developed in MIL-HDBK-217F. Each HFC-FPGA module was analyzed on a component level using the failure rate calculations for each hardware component from MIL-HDBK-217F, and the overall module failure rate was calculated from these values. The failure rates were then used to calculate availability based on a generic 28 hour Mean Time To Repair assumption at the module level. For each module, the reliability and availability values were found to be:

Table 5. Reliability and Availability Results

Module	Failure Rate 10^6/MTBF	MTBF (Hours)	MTBF (Years)	Availability
HFC-FPUD01	[			
HFC-FPUD02				
HFC-FPUA01				
HFC-FPUAO				
HFC-FPUL				
HFC-FPUM				
HFC-FPUM2				
HFC-FCPU				
HFC-FCPUX				
HFC-HSIM				
HFC-FPC08				]

These reliability and availability values were calculated for each individual module as detailed in RR901-107-02, and will be incorporated into a system-level reliability and availability analysis on a plant-specific basis.

IEEE Std 379-2000 "IEEE Standard Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems"

Testing for the HFC-FPGA modules occurred within the context of a single system. This system was designed to be part of a redundant design on a plant level. The design for each module meets the single failure requirements in this IEEE standard as well as IEEE Std 603, as the FMEA for each HFC-FPGA module found that all component failures that may affect unit performance are detectable. Single failure criterion at the system level will be evaluated at a plant-specific implementation level.

IEEE Std 384-1977 "IEEE Standard 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. As a single remote system with I/O's, only the C-Link has the capability to interface with non-safety-related equipment or controllers within the same division. The remainder of the HFC-FPGA system always remains within its own safety division.

IEEE Std 603-1991 "IEEE Standard Criteria for Safety Systems for Nuclear Power

Generating Stations"

HFC has applied the requirements established in this IEEE Std to the development process of the HFC-FPGA system. This includes the guidance from RG 1.152, RG 1.153, and NUREG-0800. The steps taken to follow guidance from these NRC RGs are detailed in Section 6.9.2. The generic system requirements for the HFC-FPGA Qualification Test Specimen were taken from EPRI TR-107330, as well as module-level requirements for voltage levels and response times. EPRI TR-107330 was used for these generic requirements, and will be re-evaluated on a plat-specific basis for any additional or changed requirements.

Single-failure criterion for the HFC-FPGA system was analyzed using Failure Modes and Effects Analysis for each module, analyzing the failure mode, possible cause, resulting effects, method of detection, and method of remediation for each component on each module.

The VV0115 Test Specimen was designed with a corresponding TSAP to simulate safety functions. The logic was verified to complete these safety functions as designed, as detailed in Section 8.2.1.

With respect to quality, the HFC-FPGA system hardware and software was designed under the QA program described in Section 6.8. This quality program has been designed, executed, and audited to follow the requirements set forth in 10 CFR 50 Appendix B, as well as IEEE Std 7-4.3.2 for software development as detailed in Section 5.4.

The HFC-FPGA system design process includes the qualification of equipment for the condition that should be specified in a plant-specific design basis to ensure system integrity. This is assured by the conservative design of the HFC-FPGA as verified during the equipment qualification testing as discussed in Section 8. However, the plant-specific boundaries would need to be affirmed before actual implementation could proceed. Timing for signal processing is another system integrity concert. The HFC-FPGA individual controller timing has been verified for the HFC-FCPU and HFC-FCPUX control modules and would need to be bounded by plant-specific analyses for each postulated event.

The HFC-FPGA qualification system is designed to function as a single division with no connections to other divisions or non-safety related systems other than through the C-Link. The C-Link communication is one-way communication through fiber optic cabling to provide the necessary electrical independence, and provides data independence using a one-way communication gateway HFC-FPC08.

For test and calibration capability, the HFC-FPGA system is designed to meet the guidance of RG 1.22 and RG 1.118. 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 able to be 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. Specific calibration and testing requirements will be evaluated on a plant-specific basis.

The only informational display presented on the HFC-FPGA system are LEDs, which can display status information and error codes. Detailed information can be obtained via EWS configuration, and will be evaluated on a plant-specific basis.

Access to the HFC-FPGA system is controlled physically during normal operation via bezel to prevent access to any ports or pins. System configuration for access control will be evaluated on a plant-specific basis.

The HFC-FPGA repair capabilities include on-line diagnostics to aid in troubleshooting as well as periodic on-line/offline surveillance procedures such as calibrations and functional testing. With modular components, repairs are done in a rapid fashion. Repair schedules and requirements will be evaluated on a plant-specific basis.

The identification of hardware and software components is controlled by HFC with its numbering system and record keeping capabilities. This is part of the HFC Configuration Management Plan. All hardware and software have a version-specific part number, and all FPGA loads have an associated build ID number. Coding of cabinets and cabling is a plant-specific item.

Reliability of the HFC-FPGA system is discussed in this section under IEEE Std 352, with the accompanying data in Table 5. Redundancy, diversity and testability which add to reliability will be addressed during the plant-specific implementation phase.

With respect to automatic control, the HFC-FPGA design meets this requirement by providing the capability to automatically actuate and control protective actions, as shown by the functions of the TSAP during qualification testing. The actual implementation will occur during the plant-specific implementation phase.

With respect to manual control, the HFC-FPGA 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.

Setpoint control for the HFC-FPGA 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 "IEEE Standard for Software Quality Assurance Plans"

The HFC-FPGA modules were designed under the quality assurance program detailed in Section 6.8. This quality assurance program is an updated version of the one used to develop the original HFC-6000 system .This software quality assurance plan is compliant with this IEEE Std as well as 10 CFR Part 50, Appendix B, and is periodically audited internally and by 3rd parties to ensure compliance.

IEEE Std 828-1990 "IEEE Standard for Software Configuration Management Plans"

The software configuration management plans used for the development of the HFC-FPGA modules are discussed in Section 5.8.

IEEE Std 829-2008 "IEEE Standard for Software and System Test Documentation"

Test documentation is discussed in the response for NRC RG 1.171 in Section 6.9.2 of this report.

IEEE Std 830-1998 "IEEE Recommended Practice for Software Requirements Specifications"

Software requirement specification guidance is discussed in Section 5.4, 5.5 and under NRC RG 1.172 in Section 6.9.2 of this report.

IEEE Std 1008-1987 "IEEE Standard for Software Unit Testing"

Software testing plans and requirements are discussed for NRC RG 1.171 in Section 6.9.2 of this report. The test documentation structure used to satisfy IEEE Std 1012 for each phase satisfies the intend of this IEEE Std.

IEEE Std 1012-2004 "IEEE Standard for Software Verification and Validation"
IEEE Std 1012-2012 "IEEE Standard for System and Software Verification and Validation"

The HFC-FPGA modules follow the guidance detailed in IEEE Std 1012-2012 for hardware, software, and systems development. The adherence to software V&V from IEEE Std 1012-2004 for the original HFC-6000 qualification has been followed and expanded upon for the HFC-FPGA modules to include part of the expanded scope of IEEE Std 1012-2012. For each phase, this includes:
Requirements Phase:

- Requirement Specification review for hardware, software, and system,
- Safety Analysis for hardware, software, and system,
- Interface Analysis for hardware, software, and system,
- Traceability Analysis for hardware, software, and system,
- Functional and In-Process Audits for hardware, software, and system,
- Configuration Management Evaluation for hardware, software, and system,
- Qualification Test Plan for hardware, software, and system,
- Acceptance Test Plan for hardware, software, and system,
- Requirements Phase Report.

Design Phase

- Design Specification review for hardware, software, and system,
- Schematic and drawing review for hardware and system,
- Safety Analysis for hardware, software, and system,
- Interface Analysis for hardware, software, and system,
- Traceability Analysis for hardware, software, and system,

- Functional and In-Process Audits for hardware, software, and system,
- Configuration Management Evaluation for hardware, software, and system,
- Integration Test Plan for hardware, software, and system,
- Qualification Test Specification for hardware, software, and system,
- Acceptance Test Specification for hardware, software, and system,
- Component Test Plan for software and system,
- Design Phase Report.

Implementation Phase

- Review of Bill of Material and artwork for hardware and system,
- Review of source code for software,
- Safety Analysis for hardware, software, and system,
- Interface Analysis for hardware, software, and system,
- Traceability Analysis for hardware, software, and system,
- Functional and In-Process Audits for hardware, software, and system,
- Configuration Management Evaluation for hardware, software, and system,
- Review of Engineering Test Plans for hardware, software and system,
- Component Test Specification for software and system,
- Review of Integration Test Specifications for hardware, software and system,
- Implementation Phase Report.

Test Phase

- Review Integration Test results for hardware, software, and system,
- Traceability Analysis for hardware, software, and system,
- Functional and In-Process Audits for hardware, software, and system,
- Configuration Management Evaluation for hardware, software, and system,
- Safety Analysis for hardware, software, and system,
- Component Test Specification execution and validation for software and system,
- Qualification Test execution and validation for hardware, software and system,
- Acceptance Test execution and validation for hardware, software and system,
- Installation Configuration Audit for software and system,
- Evaluation of User Documentation for hardware, software, and system,
- Test Phase Report.

HFC-FPGA development V&V activity also included a V&V Plan at the initiation of the project, and a final V&V Report at the end of the project. The V&V Plan for the HFC-FPGA system was generated to follow WI-VV-201, Project Verification and Validation Procedures, which merges the phase tasks in IEEE 1012 with the development phases used by HFC. The system evaluated for the scope of this project was the VV0115 Qualification Test Specimen. System V&V activity will be performed on a plant-specific basis.

IEEE Std 1016-2009 "IEEE Standard for Information Technology--System Design--Software Design Descriptions"

The HFC-FPGA software design offers the necessary information content and organization for a software design description that follows the guidance of both IEEE Stds 1016 and

1016.1. All software design descriptions and specifications were written to be highly readable and viewable with clear descriptions of component software purposes and attributes. All software design description documents for the HFC-FPGA modules include details on:

- Scope,
- References,
- Technical Design,
- System Architecture,
- Communication Interfaces,
- Timing Structure,
- Activation,
- Design Methodology,
- Software Structure,
- Design Description,
- Data Structures,
- Data Flow,
- Process Control Concepts,
- List of Software Modules.

IEEE Std 1042-1987 "IEEE Guide to Software Configuration Management"

The Software Configuration Management program for the HFC-FPGA system is discussed in Section 6.9.2 in the RG 1.169 discussion. This program is designed to comply with this IEEE Standard and was followed during the HFC-FPGA system development.

IEEE Std 1074-2006 "IEEE Standard for Developing a Software Project Life Cycle Process"

A lifecycle has been used for the design of any new FPGA software for the HFC-FPGA system, including all FPGA logic for application function. See the RG 1.173 discussion in Section 6.9.2 of this report. The overall lifecycle for HFC-FPGA modules remains unchanged from the originally qualified HFC-6000 system, with specific tasks included to meet compliance with the 2006 version of this standard and FPGA-specific tasks added to the development process as detailed in Section 5.4.

IEEE Std 1228-1994 "IEEE Standard for Software Safety Plans"

The HFC-FPGA 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-FPGA modules followed this plan for development. Training, monitoring, maintenance, event analyses and retirement are necessary issues that will be addressed during plant-specific implementation.

6.9.4 Other Documents

MIL-STD-461E "Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment"

NRC RG 1.180 calls out MIL-STD-461E as a test guidance document for EMI/RFI testing. The details and results of this testing is discussed in Section 8.2.4.2. This MIL-STD was used to EMI/RFI emissions and EMI/RFI susceptibility testing.

ASME NQA-1/NQA-1a "Quality Assurance Requirements for Nuclear Facility Applications"

The HFC quality assurance processes follow the guidance presented in these ASME standards and also meet the requirements of 10 CFR Part 50 Appendix B. Section 6.8 provides a summary of the quality assurance process for the HFC-FPGA system. This QA program is periodically audited by third party auditors to the NQA-1/NQA-1a standards.

EPRI TR-107330 "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants", December 1996

This EPRI TR was used as a basis for a generic qualification system. The VV0115 Qualification Test Specimen was designed and tested to follow the guidance in EPRI TR-107330, and Operability and Prudency testing during Equipment Qualification was based on the described test requirements in Section 5 this EPRI TR. Details of Operability and Prudency Testing are shown in Section 8.2. The harsh environmental conditions described in this TR were used as a generic qualification set of harsh environmental conditions.

6.9.5 CFR and General Design Criteria

As the GDC generally apply on a plant-specific basis, the following sections are to address these GDC that are applicable to the HFC-FPGA system.

a) GDC 1 – Quality Standards and Records

The HFC-FPGA QA procedures and record-keeping both address this requirement. The HFC-FPGA modules were designed under the QA procedures listed in the HFC QAPM and described in Section 6.8.

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

The HFC-FPGA modules were tested to seismic requirements from EPRI TR-107330, and the results of this testing are detailed in TR901-302-01, Section 10. The results of this testing show that the HFC-FPGA modules address this requirement. Details of seismic testing are shown in Section 8.2.4.5.

c) GDC 4 – Environmental and Dynamic Effects Design Bases

The HFC-FPGA modules were tested to environmental requirements from EPRI TR-107330, and the results of this testing are detailed in TR901-302-01, Section 5. Details of environmental testing are shown in Section 8.2.4.1.

d) GDC 5 - Sharing of Structures, Systems, and Components

Evaluation of the use of the HFC-FPGA across multiple parts of an installation location will be assessed on a plant-specific basis.

e) GDC 13 - Instrumentation and Control

The HFC-FPGA modules were designed and tested to this requirement across ranges anticipated for plant installations in general, using the guidance in EPRI TR-107330 as a generic set of requirements. This will be re-evaluated on a plant-specific basis.

f) GDC 19 – Control Room

The control room requirements of this GDC are supported by the HFC-FPGA system. 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.

g) GDC 20 - Protection System Functions

The HFC-FPGA modules have been designed for accommodating 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.

h) GDC 21- Protection System Reliability and Testability

HFC-FPGA system specifically addresses reliability and testability. The reliability of HFC-FPGA modules has been calculated both for Mean Time Between Failure and Availability by percentage as detailed in Table 5. All HFC-FPGA modules have an availability of 99.98% on a per-module basis. System-level reliability and availability will be evaluated on a plant-specific basis.

Testability is a primary design feature of HFC-FPGA modules. All operations being performed on the Control FPGA of a given HFC-FPGA module are checked against parallel calculations in the Diagnostic FPGA. Additionally, critical functions such as logic voltage levels, I/O point integrity, and communication are monitored by each module. Analog HFC-FPGA modules have self-calibration functionality as well. The HFC-FPGA system is able to detect and report to operators the failure or loss of communication with any single module within the system, as well as loss of redundancy. Specific aspects of testability including loss of redundancy will be evaluated on a plant-specific basis.

i) GDC 22 - Protection System Independence

Protection system independence for the HFC-FPGA system is designed to meet the requirements of this GDC. The HFC-FPGA platform has connections to other controllers and to non-safety-related equipment through the C-Link, which is discussed in more detail in Section 5.1.4. Plant-specific implementation will provide a plant-wide system level independence design that will be reviewed at that time.

j) GDC 23 - Protection System Failure Modes

HFC-FPGA modules are designed to have onboard diagnostics and a pre-determined fail-safe mode in the event of a detected failure. This includes a set failure state on loss of power, which has been tested thoroughly. The results of this loss of power test are discussed in Section 8.2.2. An assessment of each HFC-FPGA module on the component level for failure modes and the resulting effects was performed, and for each component the failure mode, possible causes, symptomatic effects, method of detection, effect of failure on the system, and method of remediation were determined.

k) GDC 24 - Separation of Protection and Control Systems

The HFC-FPGA module design ensures that there is adequate separation of protection and control systems per this criterion. All platform connections to non-safety-related equipment are via the C-Link. Electrical isolation is provided by fiber optic cabling and data isolation is through the one-way gateway. Specific isolation configurations will be evaluated on a plant-specific basis.

l) GDC 25 - Protection System Requirements for Reactivity Control Malfunctions

The HFC-FPGA system is designed to meet the requirements for reactivity control systems, including the single-failure criteria as discussed in the BTP 7-17 compliance description in Section 6.9.2. The review for this criterion will be part of the plant-specific implementation review.

m) GDC 29 - Protection Against Anticipated Operational Occurrences

HFC-FPGA based protection and reactivity control systems are designed to meet the requirements of this GDC by providing a high level of reliability and availability as described in Table 5, which can be configured for enhanced reliability and availability at the system level. System level analysis of reliability and availability are to be part of the plant-specific implementation review.

n) GDC 37 - Testing of Emergency Core Cooling System

The HFC-FPGA system has the capability to support ESFAS applications to meet this requirement with its configurations for periodic and functional testing, and the application blocks for the ESFAS application have been used and tested in the VV0115 Qualification Test Specimen. ESFAS application testing will be part of the plant-specific implementation review.

o) GDC 40 - Testing of Containment Heat Removal System

p) GDC 43 - Testing of Containment Atmosphere Cleanup Systems

q) GDC 46 - Testing of Cooling Water System

r) GDC 54 - Systems Penetrating Containment

GDCs 40, 43, 46, and 54 are supported by the HFC-FPGA system design, and will be evaluated for plant-specific implementation.

GDC 10-12, 14-18, 26-28, 30-36, 38, 39, 41, 42, 44, 45, 50-53, and 55-64 are not evaluated within the scope of this amendment, and will be assessed if applicable in a plant-specific application.

10 CFR Part 50.49 "Environmental Qualification of Electric Equipment Important To Safety For Nuclear Power Plants"

Testing of the impacts of electrical, environmental, and seismic stresses on the HFC-FPGA platform were conducted to satisfy the requirements set out in EPRI TR-107330, and are detailed in Section 8. The requirements in EPRI TR-107330 were used for a generic set of harsh conditions in place of plant-specific conditions.

10 CFR Part 50.54 "Conditions of Licenses"

The QA process detailed in Section 6.8 meets the requirements set forth in section (jj). The remaining portions of 10 CFR Part 50.54 will be evaluated on a plant-specific basis.

10 CFR Part 50.59 "Changes, Tests and Experiments"

All HFC-FPGA modules are strictly version-managed and will only be updated for an on-site application following the SCR change process detailed in Section 9.0. This change process is designed to ensure all safety analyses and regression tests are correct, complete, and valid before any changes to site equipment are made.

10 CFR Part 52.47 "Contents of Applications; Technical Information"

All HFC test procedures have explicitly stated acceptance criteria, as required in (b)(1). All test results are evaluated against these acceptance criteria. Other portions of 10 CFR Part 52.47 will be evaluated on a plant-specific basis.

6.10 DEFENSE-IN-DEPTH AND DIVERSITY EVALUATION PROCESS

The HFC-FPGA modules are designed to function in the same manner with respect to defense in depth as the HFC-6000 qualified system, in that diversity will be evaluated on a plant-specific basis. The HFC-6000 system's compliance with Defense-In-Depth requirements is detailed in PP901-000-01, Section 8.6. These are:

6.10.1 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.

6.10.1.1 Compliance with 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. 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-FPGA 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.

6.10.2 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.

6.10.2.1 Compliance with Position 2:

To simplify the defense-in-depth and diversity analysis, postulated common-mode failures of the HFC-FPGA 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-FPGA 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 basis at a later date.

6.10.3 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.

6.10.3.1 Compliance with 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 updated final safety analysis report. 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-FPGA safety system will be configured to enhance the plant's defense-in-depth and diversity with specific techniques such as critical analog signals and critical manual signals, which will be evaluated on a plant-specific basis.

6.11 CYBER SECURITY

6.11.1 Vulnerability Assessment

The identification of potential security vulnerability in the development life cycle phase focuses on security intrusion threats. The HFC V&V team conducted security analysis at applicable life cycle phases and documented the security vulnerabilities in the development life cycle phases. Control measures were used to address those identified vulnerabilities. The vulnerabilities in the development life cycle phases of the HFC-FPGA modules were determined to be comparable to those for the original HFC-6000 platform. A summary of these vulnerabilities by phases was found to be:

Requirements Phase:
- Unauthorized updates to documents,
- Uncontrolled versions of documents.

Design Phase:
- Unauthorized updates to documents,
- Uncontrolled versions of documents,
- Unnecessary or unaddressed design criteria or functions.

Implementation Phase:
- Unauthorized updates to source code, schematics, or drawings,
- Uncontrolled versions of source code, schematics, or drawings,
- Unnecessary code or hardware features,
- Unaddressed requirements.

Test Phase:
- Unauthorized changes between Implementation and Test Phase versions,
- Product release without complete testing,
- Unaddressed or untested functions and features.

The vulnerability assessment for the operational phases of HFC-FPGA modules also focused on cyber security based intrusions and faults, and the HFC-FPGA platform has been designed to block outside cyber security threats. The HFC-FPGA platform uses the HFC proprietary F-Link, G-Link and RIF as internal communication links, which have a pre-defined message structure, size and timing, and will log any message in the link that deviates from the required size, structure and source as errors, in a manner similar to the

HFC-6000 ICL. Additionally, the only external communication link for the qualified HFC-6000 system and the HFC-FPGA modules addressed in this amendment is the C-Link. These appropriate security design features are included in the design to address intrusion threats, hence to protect the reliable operation of the system from undesired behavior from connected systems. Due to the technical difference between the original microprocessor based HFC-6000 platform and HFC-FPGA platform, the specific security design concept and features for HFC-FPGA modules and system were evaluated separately and an FPGA-specific safety concept was generated. Security concepts for the HFC-FPGA modules not only addressed the vulnerabilities identified, but also met the regulatory requirements posed by Regulatory Position 2.1 (no remote access to the safety system) and Regulatory Position 2.3.1 (only one-way communication from safety system to other lower level system) of RG 1.152. Each communication pathway has been analyzed for security vulnerabilities with design steps taken to mitigate these vulnerabilities, including predefined communication node, format, timing and mastership handling mechanisms to effectively block intrusion from an external system. System-level cyber security will be evaluated further on a plant-specific basis.

6.11.2 Secure Development and Operational Environment Controls

HFC established a cyber security program in accordance with the regulatory requirements and guidance contained in RG 1.152, NRC NUREG-0800, IEEE Std 7-4.3.2, IEEE Std 1012, IEEE Std 828, NIST 800-53 and NIST 800-82. Security controls for a safety-related system development and operational environment were developed after a risk assessment of the HFC-FPGA system. This includes the identification of critical digital assets, development of defensive safeguards for these critical digital assets, and testing to ensure the safeguards in place are functioning as required. Version management, password protection, physical access control, and checksum verification are examples of safeguards in place to protect the development environment and other critical digital assets. The HFC-FPGA system development was performed under a platform-generic cyber security plan, which included re-evaluation of the effectiveness of safeguards during each phase of development. Implementation and execution of security controls and measures in the cyber security guideline and cyber security plan ensure that identified vulnerabilities in the development life cycle phases are properly addressed. The HFC-FPGA platform is designed with appropriate security concept to block potential outside intrusion threat in the operational phases and promote runtime reliability of HFC-FPGA platform. Plant-specific operational environments will be evaluated on a plant-specific basis.

6.12 ISOLATION AND INDEPENDENCE

The HFC-FPGA system is structured as a collection of safety-related devices 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 through a fiber optic cable and an isolation gateway. Furthermore, there are no inter-channel or inter-divisional connections within the HFC-6000 for the original qualified system or the HFC-FPGA system. However, these connections could be provided during a plant-specific implementation. The actual details for acceptable isolation and independence for these areas will be provided during this plant-specific implementation.

7.0 TOOL USE AND QUALIFICATION

All tools used in the development of FPGA modules for the HFC-FPGA system were controlled and tested as required in IEEE Std 7-4.3.2. All tools used in the development process were subject to HFC's configuration management program, which follows the guidance in 10 CFR 50 Appendix B, as detailed in Section 6.8. Additionally, each tool follows one or both of the methods outlined in IEEE Std 7-4.3.2: an individual tool validation program, and/or testing to ensure defects are detected by V&V activities.

7.1 TOOL QUALIFICATION METHODOLOGY

The guidance specified in IEEE Std 7-4.3.2-2003 requires that software tools used to support software development processes and V&V processes shall be controlled under configuration management. One or both of the following methods shall be used to confirm the software tools are suitable for use: 1) A test tool validation program shall be developed to provide confidence that the necessary features of the software tool function as required. And 2) the software tool shall be used in a manner such that defects not detected by the software tool will be detected by V&V activities. Finally, tool operating experience may be used to provide additional confidence in the suitability of a tool, particularly when evaluating the potential for undetected defects. Several HFC tools such as the SOE and HAS utilities have significant operating experience in safety and non-safety applications.

International Atomic Energy Agency (IAEA) Nuclear Energy Series, No. NP-T-3.17 also provides guidance for the use of software tools. Per the IAEA technical report, "Most national regulatory bodies require that all tools that will be used to perform safety functions or that are used in the development process for hardware, software or firmware to perform a safety function be treated as safety software (method II in Figure 21). This can be a significant regulatory burden for pre-developed software tools used in any digital system development cycle. Tool developers typically do not provide detailed evidence of their configuration management for their tools or the level of error tracking and quality assurance needed to support and maintain their tools as safety grade software for nuclear power plant applications."

"The alternative method that has been found acceptable to most regulatory bodies is to independently review the input and output of tools as part of the development process quality assurance program to ensure that the tool is functioning properly, and that it has not introduced any possible new fault or failure mode into the final digital system or failed to detect an error if that is part of the function of the tool. Owing to the challenges with method II, this method (method I in Figure 21) is more commonly used at the current time. When tools are used for specific, well bounded parts of the development process, method I has proved to be effective."

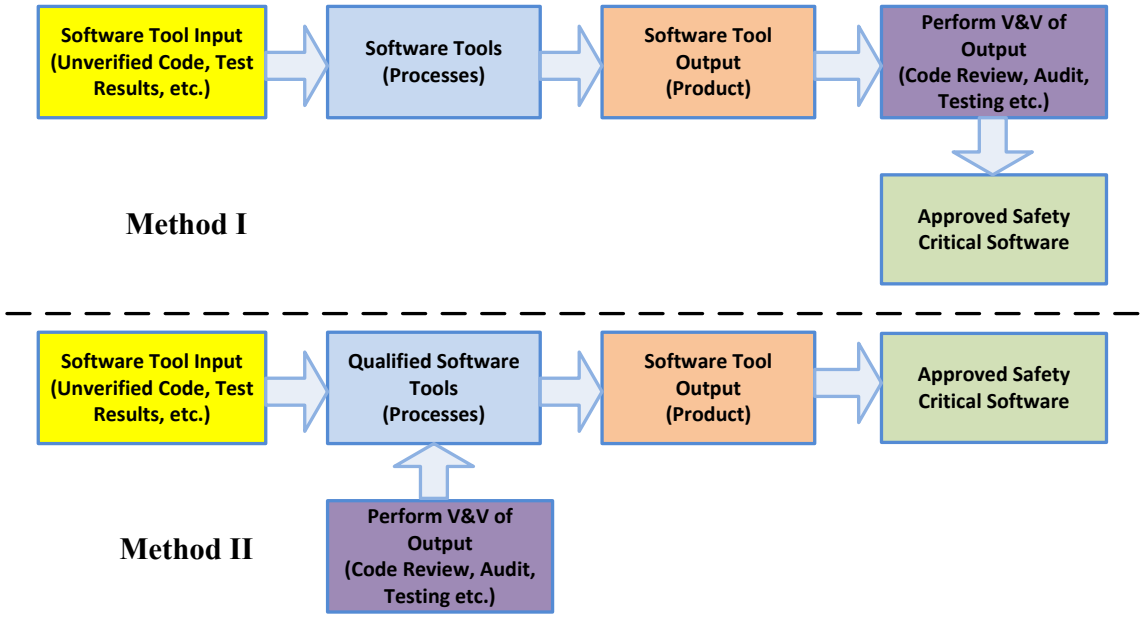

Figure 21. Two Acceptable Methods for Tool Qualification

7.2 QUALIFICATION OF ONE-STEP

When using HFC-FPGA system for Reactor Protection System (RPS) or Engineered Safety Features Actuation System (ESFAS) applications, the RPS and ESFAS implementation starts with plant-specific requirements and licensing basis, which are translated into system requirements specification and followed by the system architectural design. The system design and architecture implementation are then realized via the generic FPGA platform, where the RPS and ESFAS applications logics are executed.

To execute the RPS and ESFAS applications logics, logic drawings or diagrams are first translated into HDLs. Then, using an electronic design automation tool, a technology-mapped netlist is generated; this synthesis process translates HDL or schematic design to logic gates, memory units, registers and connections. The netlist can then be implemented by the FPGA manufacturer's proprietary tool (e.g. Libero) to fit to the actual FPGA architecture. This includes translation, map and place-and-route processes. The designer as well as V&V engineers will verify the map, place-and-route results via timing analysis, simulation, and other verification methodologies. Once the design and verification process is complete, the programming file generated (also using the FPGA manufacturer's proprietary tool) is employed to (re)configure the FPGA. This file is transferred to the FPGA via a serial interface (JTAG).

The process of translating logic drawings into the HDLs is laborious and error prone, especially for a system with a great number of inputs and outputs. It is therefore desired to automate the translation process, and achieve error-free implementation and execution of safety logic algorithms. For this reason, One-Step for FPGA applications has been developed by HFC. The One-Step software tool not only automates the logic translations but also creates dynamic indication of a CAD (Computer-Aided Design) drawing for display on the workstations so that logic drawings can be dynamically monitored with the system on-line.

HFC implements a V&V program in validating tools for use in FPGA applications. This program is consistent with the guidance provided by the IEEE Std 7-4.3.2-2003 and the V&V methodologies specified in the IEEE Std 1012-2004 to evaluate and qualify tools before they are used. The IEEE Std 1012-2004 requires tools that insert code into the software be verified and validated to the same rigor as the highest software integrity level of the software.

The qualification of HFC-FPGA platform One-Step therefore consists of the following steps: tool requirements specification development, tool detailed design and implementation, tool V&V program, tool revision control and the use of the tool in nuclear safety I&C applications.

The tool V&V program includes specific steps as follows:

- Review and Verification of Tool Requirements Specification and Design Implementation,
- Tool Code Review and Walkthrough,
- Tool Code Coverage Testing (complete for all needed logics gates and Macros),
- Tool Functional Coverage Testing (all logics functions),
- Tool Functional and Timing Simulation Testing (on all required logics and selected examples), and
- Tool Use in the FPGA Circuitry System Testing (on selected typical applications as well as loops logics that have been used in operating NPPs).

After the logic is converted into the HDL file, as part of the One-Step process, the FPGA manufacturer's proprietary tool and IP core components are used to generate the programming file, which is employed to (re)configure the FPGA. This file is transferred to the FPGA via a serial interface (JTAG). The programmed FPGA based control system is then verified and validated via system testing.

Additionally, the proven microprocessor based One-Step was used to verify and validate the correctness of the end results from the FPGA based applications (See Figure 22).

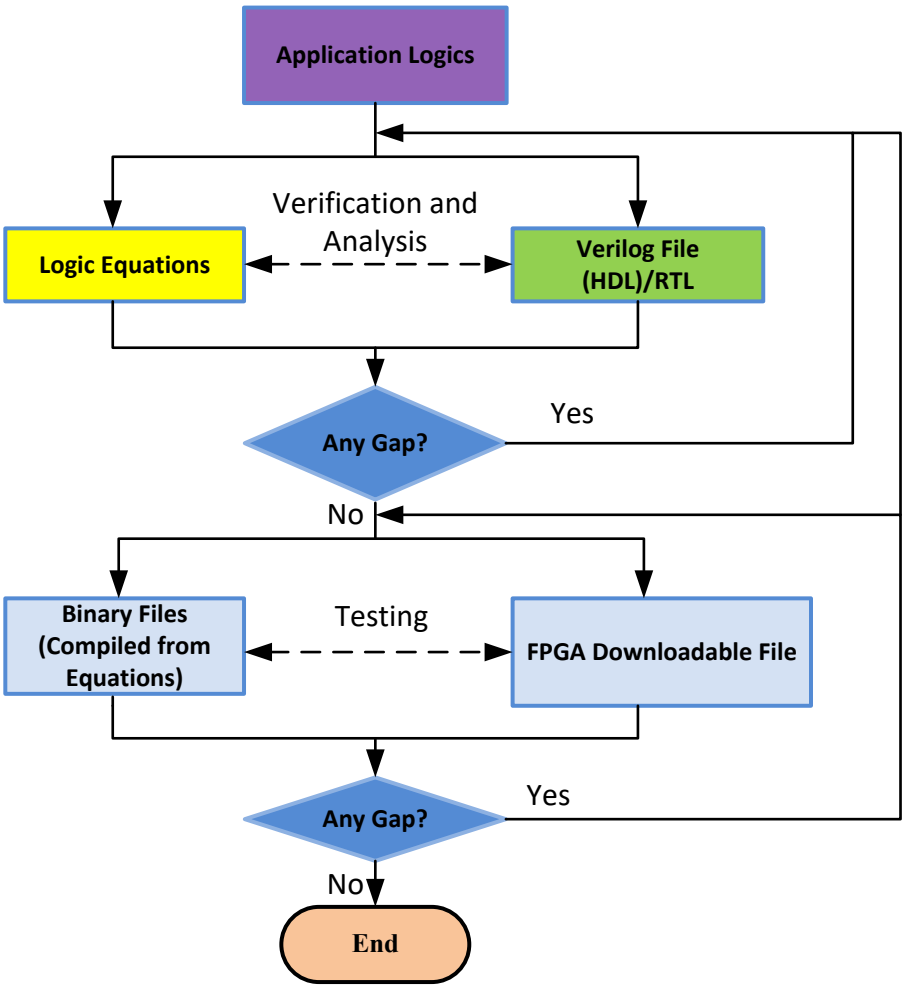

Figure 22. Additional Approach to Ensure the Correctness of FPGA One-Step

This approach for using the proven history of the One-Step for microprocessor based applications provides additional confidence that the One-Step tool for FPGA applications generates correct results and does not mask errors.

7.3 QUALIFICATION OF OTHER THIRD PARTY FPGA TOOLS

While the HFC One-Step tool development followed Method II as shown in Figure 21, the qualification of third parties' tools in the application of FPGA follows Method I as shown in Figure 21. This complies with the IEEE Std 7-4.3.2 clause 5.3.2 that "the software tool shall be used in a manner such that defects not detected by the software tool will be detected by V&V activities." Tools verified in this way include Libero, FlashPro, and IP Cores utilized in FPGA design.

8.0 EQUIPMENT QUALIFICATION

The HFC-FPGA system underwent equipment qualification in accordance with RG 1.209 as a generic platform. Harsh environmental conditions as specified in EPRI TR-107330 were applied to the VV0115 Test Specimen. This test specimen was designed to follow the guidance in EPRI TR-107330 for defining a generic system, TSAP, and acceptance criteria for normal performance. As the HFC-FPGA platform had no plant-specific harsh environmental conditions, the generic qualification envelopes set forth in EPRI TR-107330 for environmental stress and seismic were used as a generic set of harsh environment conditions. Requirements defined in NRC RG 1.180 were used as the basis for EMI/RFI, ESD, and surge withstand qualification tests. Testing for these modules was performed at three locations: HFC's location in Carrolton TX, Environmental Testing Laboratory in Dallas TX, and National Technical Systems in Plano TX.

8.1 SYSTEM QUALIFICATION TESTS

8.1.1 Scope

The Qualification Test Specimen was designed to function as a representative example of an HFC-FPGA system, containing all modules listed in Table 1 operating as they would in a plant. The TSAP used for the Qualification Test Specimen was developed to follow EPRI TR-107330 to demonstrate capabilities comparable to those that would be required on a plant-specific basis. The qualification process was:

a) The HFC-FPGA modules listed in Table 1 were designed and assembled following HFC's QA program and applicable Work Instructions.

b) The Qualification Test Specimen was designed and assembled using at least one instance of each HFC-FPGA module from Table 1 in a representative configuration. Support equipment was included to interface with the HFC-FPGA modules in a manner comparable to how they would be implemented in a plant setting.

c) The TSAP was defined and developed for HFC-FCPU and HFC-FCPUX modules of the Qualification Test Specimen. This TSAP served as a synthetic application designed to aid in the qualification and operability tests for the test specimen. In place of plant-specific requirements for the application, guidance from EPRI TR-107330 was used for defining the parameters of the TSAP.

d) The HFC-FCPU, HFC-FCPUX, HFC-FPGA I/O modules, and the TSAP were combined into a test configuration for execution of acceptance tests. This activity constitutes the system integration testing for each module included in the Qualification Test Specimen. This assembly was named the VV0115 Test Specimen, and the design is detailed in VV901-300-10 including applicable support equipment and external wiring.

e) A set of qualification tests to be performed on the Qualification Test Specimen was created, including a defined set of Operability and Prudency tests to be conducted periodically during the qualification process. Operability and Prudency testing was

performed before all qualification testing, after environmental testing, after EMI/RFI testing, and after seismic testing. This was done to assess the impact of each group of tests on Test Specimen performance. A top-level description of these tests is shown in Figure 23.

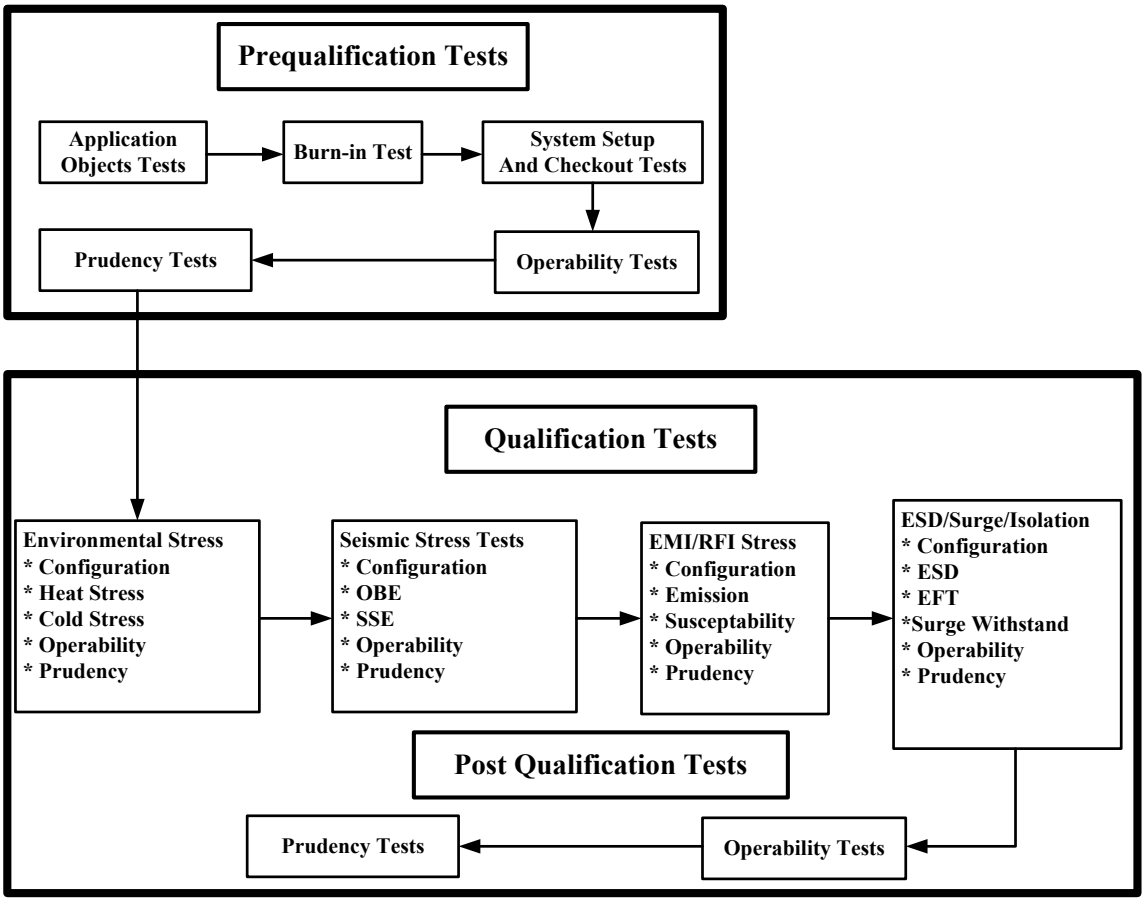

Figure 23. Overall Test Arrangement and Sequence

f) The qualification tests were performed, and the results were retained, analyzed for compliance with the acceptance criteria, and documented. A full report of qualification test results including completed procedures is given in TR901-302-01. Baseline testing was performed periodically during the test sequence in Figure 23 to monitor for impacts on performance of the Qualification Test Specimen.

This test program intentionally duplicated the overall testing conducted for the original qualification of the HFC-6000 Safety Platform in order to demonstrate that the new FPGA hardware and software design will meet or exceed the capabilities of that platform. The specific sequence of EMI/RFI testing was not replicated due to the availability of laboratory equipment, and additional Operability and Prudency testing was performed relative to the original HFC-6000 qualification testing to obtain more information about the impacts of specific tests on the Test Specimen.

8.1.2 Equipment Tested

A set of the newly developed HFC-FPGA modules as described in Table 1 was assembled into a test specimen. A block diagram representation of this Qualification Test Specimen is shown in Figure 2. The test specimen is configured to be a generic platform, using the functionally specified in EPRI TR-107330, Section 4 in place of plant-specific operating requirements. The overall test specimen includes sufficient functional capabilities to encompass a significant range of applications.

The system layout drawings, wiring and power distribution diagrams, and assembly diagrams define specific details of the hardware design for the test specimen. Test plans and procedures provide detailed requirements and instructions for equipment mounting and interfaces to be used for equipment testing. The TSAP for each HFC-FCPU and HFC-FCPUX controller was developed as new application code using PromisE software and following the HFC Application Development process including the review and version management process required by the HFC QAPM. Table 6 contains the Master Configuration List of equipment used in the VV0115 Qualification Test Specimen. Table 6 also describes the functions of each module that were tested by the Qualification Test Specimen.

Table 6. Qualification Test Specimen Items

Rack Plug-In PCBs		
Designation	**Part Number**	**Function**
HFC-FPUD01	[	
HFC-FPUD02		
HFC-FPUA01		
HFC-FPUAO		
HFC-FPUL		
HFC-FPUM		
HFC-FPUM2		
HFC-FCPU		
HFC-FCPUX		
HFC-HSIM		
HFC-FPC08		]
CON Cards (Plugs in at rear of backplane slots for interface to Termination Cards)		
Designation	**Part Number**	**Function**
HFC-FPC08CON4	[	]

HFC-FPUDCON	[	
HFC-AI16CON2		
HFC-AO8CON2		
HFC-AI8CON2		
HFC-HSIMCON 1300nm 2RX		
HFC-HSIMCON 1300nm 2TX		
HFC-AI8CON3		
HFC-FCPUCON		]
Termination Cards (Field wire connection point. Connected to CON cards via DB25/50 cables)		
Designation	**Part Number**	**Function**
HFC-TBDO16T4	[	
HFC-TBDI16T3		
HFC-TBAI8LT		
HFC-TBAI8MT		
HFC-TBAO8T		
HFC-TBAI16T		]
Miscellaneous Equipment		
Designation	**Part Number**	**Function**
CABLE ASSEMBLY, DB50, 9 FOOT S10097, TYPE A	[	
CABLE ASSEMBLY, DB25, 9 FOOT S10096, TYPE A		
HFC-FOT06		
RIF Cable		
HFC-BPE01-19		]

Detailed configuration information, a full list of included hardware, and a detailed description of the TSAP is described in VV901-300-10.

All FPGA used on the HFC-FPGA system were designed and manufactured by Microsemi, from the IGLOO, IGLOO2, and ProASIC3 product lines. The specific Microsemi FPGA chip used in each module is listed in Table 7:

Table 7. FPGA Type and Quantity

Module	FPGA Used	Quantity of FPGA used
HFC-FPUD01	[	
HFC-FPUD02		
HFC-FPUA01		
HFC-FPUAO		
HFC-FPUL		
HFC-FPUM		
HFC-FPUM2		
HFC-FCPU		
HFC-FCPUX		
HFC-HSIM		
HFC-FPC08		]

8.1.3 Safety Functions Tested

The Qualification 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 are as follows:

a) The capability of the test specimen to perform defined design functions within specified tolerances under normal environmental and operating conditions. Performance was measured using:
   - Response Time for digital and analog I/O points,
   - Digital and analog I/O point operability,
   - Fault detection capability,
   - Fault recovery capability,
   - Redundancy and failover operability,
   - External communication via RS-485.

b) 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 seismic stress,
   - Function during and after application of EMI/RFI waveform exposures,
   - Function during and after application of ESD/EFT/burst test discharges,
   - Function during and after exposure to surge test waveforms.

These functional capabilities were selected to exercise the system in a manner comparable to a plant application.

8.1.4 Test Requirements

The qualification for the integrated test specimen consisted of a set of prequalification tests, a set of qualification tests, and a set of post-qualification tests as illustrated in Figure 23. These tests served two primary purposes:

- Tests conducted prior to the start of qualification testing confirmed that both 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 as a whole. 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 harsh conditions as defined in EPRI TR-107330 and NRC RG 1.209. The purpose of these tests is to demonstrate the capability of the system hardware and software to continue operating within specified tolerances under extreme conditions. The full Operability and Prudency tests were run in between different qualification tests (Environmental EMI/RFI, Seismic) to more accurately assess the effects of each specific test on the Test Specimen.

8.1.4.1 Test Procedures

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

- TP901-200-01 EPRI TR-107330 Burn-in Test Procedures,
- TP901-115-05 VV0115 Integration (Set-up and Check Out) Test Procedure,
- TP901-115-06 VV0115 TSAP Validation Test Procedure,
- TP901-115-01 VV0115 Qualification Operability Test Procedure,
- TP901-115-02 VV0115 Qualification Prudency Test Procedure,
- TP901-302-02 VV0115 Qualification Environmental Stress Test Procedure,
- TP901-302-03 VV0115 Qualification EMI RFI Test Procedure,
- TP901-302-04 VV0115 Surge Withstand Test Procedure,
- TP901-302-05 VV0115 Electrostatic Discharge Withstand Test Procedure,
- TP901-302-06 VV0115 Qualification Seismic Test Procedure.

A master test plan was generated to provide a link between the guidance of EPRI TR-107330, NRC Regulatory guides, and the procedures that were used to conduct the tests. The test plan addresses the general approach for the test program, as detailed in VV901-300-09. Two types of application programs are associated with the testing effort defined by these test plans:

- Test Specimen TSAPs for the HFC-FCPU and HFC-FCPUX controllers, and
- HFC Plant Automated Tester (HPAT) program for the test workstation.

HFC uses both a Sequence of Events (SOE) utility and a Historical Archiving System (HAS) utility to log data generated during a test program. Both the SOE and the HAS are

HFC proprietary utilities that were developed to operate with HFC control systems. The SOE utility resides on a set of special DI modules configured for a separate controller associated with the HPAT. This utility has a resolution of ±1 ms and is used to record high-speed transitions of digital data points. An HFC proprietary program residing on the HPAT test computer is used to transfer the logged data from the buffer in the DI modules to text files during the test period. The contents of these text files are subsequently imported into MS Excel files for analysis and evaluation.

The HAS utility logs configured data points into an SQL database that resides in the HPAT test computer. The data can later be extracted from the SQL database for processing. Each record in this database includes a time stamp as well as a point ID. These parameters permit construction of queries to extract specific data relating to each test individually. The results of these queries are copied to separate MS Excel files for analysis and evaluation.

8.1.4.2 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., environmental, seismic, and EMI/RFI/ESD/EFT testing) were conducted for HFC by personnel at qualified test facilities. HFC test personnel were present and conducted specified portions of the Operability and Prudency tests during these qualification tests.

8.1.4.3 System Operational Stress Conditions

EPRI TR-107330, Paragraph 6.3.1 identifies the major aging factors to be considered in system qualification. The following sequence of tests exposes the qualification system to conditions that simulate the following stress factors:

- Environmental stress test. This test exposes the test specimen to abnormal combinations of high/low temperature and humidity.

- Seismic stress test. This test exposes the test specimen to high amplitude inertial forces.

- Electromagnetic Interference/Radio Frequency Interference (EMI/RFI) test. This includes two aspects:
  a) It measures the amplitude of electromagnetic energy radiated by the system over specified frequency ranges; and
  b) It tests the system for functional susceptibility to EMI/RFI from external sources.

- Electrostatic Discharge test. This test verifies that the system continues operating normally during and after application of ESD pulses to specified locations.

- Surge Withstand/EFT/Burst Immunity tests. These tests apply large amplitude transient pulses having different characteristics to various points of the system to establish the level of operational immunity built into the system hardware.

Each test exposes the test specimen to harsh conditions while it is powered up and running the TSAP. The EPRI specification and Regulatory Guides provide 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 as shown in in Figure 23.

8.1.4.3.1 Environmental Stress Qualification

Environmental stress qualification test levels for temperature and relative humidity were determined from EPRI TR-107330, with a 5% margin added. These conditions were used as a generic harsh environmental condition, in place of plant-specific measured conditions. The purpose of this test was to demonstrate that the physical components of the test specimen work within acceptable parameters including timing and maintaining contact during heating and cooling. Environmental conditions for this test are shown in Figure 24.

8.1.4.3.2 Seismic Withstand Qualification

Seismic withstand qualification levels and test sequence were determined from EPRI TR-107330 and NRC RG 1.100. This test consists of five consecutive OBE cycles and one SSE cycle. The purpose of this test was to demonstrate that the physical components on the PCB assemblies, mechanical junctions, and cable assemblies remain in place and operational during and after application of significant inertial forces. Seismic spectrum levels are shown in Figure 25.

8.1.4.3.3 EMI/RFI Qualification

EMI/RFI qualification levels were determined from NRC RG 1.180. For radiated and susceptibility tests, the MIL-STD-461E methods were used to determine the appropriate testing levels. The purpose of these tests was to demonstrate that the components of the test specimen would not emit significant EMI/RFI noise that could interfere with the operation of nearby plant equipment, and that it was not susceptible to the level of EMI/RFI noise likely to be present in a plant environment.

8.1.4.3.4 Surge Withstand Qualification

Surge Withstand qualification levels were determined from NRC RG 1.180. The IEC method for Surge Withstand Capability was used to determine the appropriate test signal levels and waveforms. The purpose of these tests was to demonstrate that the components of the test specimen would perform without significant disruption from the injection of these waveforms.

8.1.4.3.5 Electrostatic Discharge Withstand Qualification

Electrostatic Discharge Withstand qualification levels were determined from IEC 61000-4-2. This standard was selected to determine the appropriate test signal levels and testing methodology to demonstrate the ability of the test specimen to perform without significant disruption when exposed to ESD signals likely to be found in a generic industrial environment.

8.2 SYSTEM QUALIFICATION TEST RESULTS

8.2.1 Prequalification Tests

The Prequalification Tests consist of the Application Objects Test, Burn-In Test, System Setup and Checkout Test, and TSAP Validation Test. These tests were taken from EPRI TR-107330, Section 5.2 to verify that the Qualification Test Specimen performed as designed. TR901-302-01 Section 4 details the results of prequalification testing, all of which were found to be within the required acceptance criteria.

8.2.2 Operability Tests

The following set of Operability tests was performed following completion of the TSAP tests. The purpose of these operability tests is 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.

- **Accuracy Test** - This test develops a baseline to compare against the accuracy and linearity of the analog I/O modules observed during the qualification tests. The AI and AO accuracy acceptance criteria are ±0.35% of full range.
- **Response Time Test** - This test measures the response time for discrete and analog inputs from the leading edge of the input to the leading edge of the resulting output. The acceptance criteria for response time are 100 ms for digital logic, and 300 ms for analog logic.
- **Discrete Input Operability Test** - This test verifies the capability of discrete input channels to detect a transition in the input signal being monitored. The acceptance criteria for digital inputs are 12V to 15V set and dropout level, and 53V maximum input voltage.
- **Discrete Output Operability Test** - This test verifies the capability of discrete output channels to operate reliably within their specified loading conditions. The acceptance criteria for digital outputs are 24 VDC excitation voltage.
- **Communication Operability Test** - This test verifies reliable data transfer over the F-Link, RIF, and G-Link. For all three links, the acceptance criteria are that no disruption of I/O scanning or module-to-module communication occurs.
- **Timer Test** - This test develops the baseline for the timer function accessible to the TSAP. Acceptance criteria of this test are the continued accurate performance of a 1-second and 5-second timer during operability testing.
- **Failure to Complete Scan Test** - This test demonstrates that the system will detect an incomplete scan within one controller operation cycle. The acceptance criteria for this test are that an incomplete scan will be detected within 300 ms, logged as an event, and will not vary by more than 10% across qualification testing.
- **Loss of Power Test** - This test demonstrates correct response of all I/O channels to a loss of source power followed by reapplication of power to the system. The acceptance criteria for this test are that all output channels deenergize on loss of power, and return to the defined failsafe state on return of power.
- **Power Interruption Test** - This test demonstrates the capability of the power modules to sustain system operation during a temporary (40-ms transient) source

power interruption. As the power supplies used for the VV0115 Test Specimen were already qualified for use with the HFC-6000 system, this test was not repeated.

All tests were performed in accordance with their respective Operability Test procedure for the VV0115 Test Specimen, and evaluations of each instance of the Operability Test conducted were detailed in TR901-302-01 in the applicable qualification test section. Overall, Operability testing showed that the Test Specimen operated within the acceptance criteria before, during, and after all Equipment Qualification tests.

8.2.3 Prudency Tests

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, exercise the test specimen in various ways to simulate controller loading. All Prudency tests were executed during the prequalification phase of testing to establish a performance baseline for the test specimen. The following specific tests were defined:

- **Burst of Events (BOE) Test** - This test is configured to impose a large number of operations on the HFC-FPGA test specimen simultaneously. This test is automated and is typically run as a continuous background operation for selected qualification tests. The Burst of Events test changed states of the points in Table 8 at a 1 Hz frequency.
- **Serial Port Failure Test** - The test specimen has just one redundant serial communication link connected to all of the modules under test and two additional serial links associated with the HFC-FCPU and HFC-FCPUX modules. This test imposed three simulated failures on a single channel of the redundant links, 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 requires introduction of a 100 kHz sawtooth noise signal at 2.5 Vrms signal on the serial link one port at a time.
- **Fault Simulation Test** - This test requires introduction of a simulated failure condition in the primary controller to trigger failover to the secondary controller. The coverage of this testing was met by failover testing as performed by the Operability Test, and was not repeated for Prudency testing.

Table 8. Burst of Events Points

[

]

All tests were performed in accordance with their respective Prudency Test procedure for the VV0115 Test Specimen, and evaluations of each instance of the Prudency Test conducted are detailed in TR901-302-01. Overall, Prudency testing showed that the Test Specimen operated within the acceptance criteria before, during, and after all Equipment Qualification tests.

8.2.4 Qualification Tests

The Qualification Tests consist of the following tests: Environmental, Seismic, EMI/RFI, ESD, and Surge Withstand/EFT/Burst Immunity tests. 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. During all qualification testing, the Automated Accuracy, Automated Response Time, Bust of Events, and Timer tests were run, and the results were compared against the acceptance criteria listed in Section 8.2.1. For all qualification tests, the Test Specimen was found to meet these acceptance criteria.

8.2.4.1 Environmental Stress Qualification Tests

The selection of what components were to undergo environmental qualification testing and overall method for that qualification testing was determined using the guidance in RG 1.209. EPRI TR-107330 states that the environmental stress test is to be the first of the qualification tests to be conducted. This test exposes the VV0115 Qualification Test Specimen of the HFC-FPGA system to extremes of temperature and humidity in order to induce accelerated aging of functional components. It was accomplished by enclosing the Test Specimen in an environmental test chamber. The Test Specimen was running the TSAP throughout the test period, and its operation was monitored by SOE and HAS data loggers located outside the test chamber. In addition, comprehensive functional tests 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 24):

[

]

As specified in EPRI TR-107330, operability checks or validation tests are required at various points during the test to ensure that the platform continues to operate normally. The specific test period minimum durations are depicted in Figure 24.

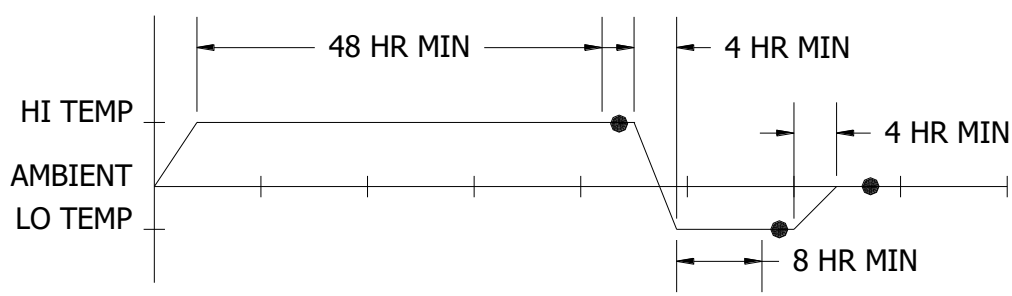

Figure 24. Environmental Stress Test Profile

Note: The black dots on the graph designate the operability check points required by the EPRI standard.

High humidity (95%) during high temperature and low humidity (0%) during low temperature were maintained. For all automated tests performed during the high temperature, low temperature, and transition times, SOE and HAS data shows that the automated tests being run continued to operate within the acceptance criteria. During the high temperature, low temperature, and ambient operability tests all conducted tests met the acceptance criteria as well. Details of the results of this test are discussed in TR901-302-01, Section 5.

8.2.4.2 EMI/RFI Qualification Tests

The HFC-FPGA VV0115 Test Specimen was 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 both the susceptibility of the Test Specimen to EMI/RFI noise and the magnitude of EMI/RFI noise generated by the Test Specimen. All emissions profiles and susceptibility signal levels were selected to conform to the requirements of RG 1.180.

- The emissions tests RE101, RE102, CE101, and CE102 were performed with the Automated Operability and Burst of Events tests running to simulate normal equipment activity. During all emissions testing, the Test Specimen met the acceptance criteria for emissions profiles and Test Specimen performance. Emissions limits set forth in RG 1.180 Section 3 were used for these tests.
- The susceptibility tests RS101, RS103, CS101, CS114, CS115, and CS116 were performed with the Automated Operability and Burst of Events tests running to simulate normal equipment activity. During all susceptibility tests, the Test Specimen met the acceptance criteria. Test levels and operating envelopes set forth in RG 1.180 Section 4 were used for these tests.

The test specimen met acceptance criteria during all emissions and susceptibility tests. Details of this testing are discussed in TR901-302-01, Section 8.

8.2.4.3 ESD Test

Components of an HFC-FPGA 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 subjected each component of the HFC-FPGA Test Specimen to simulated ESD pulses to establish their capability to withstand such discharges without disabling or disrupting normal operation. Detailed requirements for ESD immunity were defined by IEC 64000-4-2:

- Contact discharge levels were 8 kV, applied ten times at a positive polarity and ten times at a negative polarity to each test point.

- Air discharge levels were 15 kV, applied ten times at a positive polarity and ten times at a negative polarity to each test point.
- All HFC-FPGA module toggle switches and bezels were subjected to ESD testing.
- Points on the VV0115 Test Specimen found to be likely contact points such as power supply switches, tie bars, and mounting screws were subjected to ESD testing.

Overall acceptance criteria were as follows:

- Subjecting the system to the specified level of ESD shall not disrupt operation or cause damage. The automated Operability and Prudency tests were used to evaluate the operation of the Test Specimen and its normal operation.
- For redundant platforms, performance is satisfactory if the platform performs as intended after being subjected to the specified level of ESD.

The test specimen met all acceptance criteria for all points tested. Details of the test results are discussed in TR901-302-01, Section 9.1 and 9.2.

8.2.4.4 Surge Withstand/EFT/Burst Immunity Test

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 injects 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 remain within acceptable limits during and after exposure to such discharges. The Test Specimen was powered on and running the TSAP and automated Operability and Prudency tests when the test pulses are being applied to specific circuits in accordance with RG 1.180 Section 5. Four tests were conducted:

- Ring Wave per IEC 61000-4-12, Category B at 4 kV applied to 120 VAC input power.
- Combination Wave per IEC 61000-4-5, Category B at 4 kV / 2 kV applied to 120 VAC input power.
- EFT per IEC 61000-4-4, Category B at 4 kV applied to 120 VAC input power.
- EFT per IEC 61000-4-4 at 500 V, coupled into signal lines.

Overall acceptance were as follows:

- Application of surge waveform shall not damage any other, component, or channel other than those specific modules or circuits under test.
- Channels or modules other than the one under test 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.
- Automated Operability and Prudency tests continue to run and meet their acceptance criteria during the application of test waveforms.

The Test Specimen met all acceptance criteria during the Ring Wave, Combination Wave, and EFT testing. Details of the test results are discussed in TR901-302-01, Section 9.3.

8.2.4.5 Seismic Stress Test

Seismic testing exposed the Test Specimen to a set of dynamic spectra designed to simulate an Operating Basis Earthquake (OBE) and a Safety Shutdown Earthquake (SSE) in accordance with the guidance from RG 1.29. This test spectrum defined by EPRI TR-107330 is shown in Figure 25. The dynamic spectra consist of tri-axial, random, multi frequency waveforms that are transmitted to the Test Specimen by means of hydraulic actuators attached to a Seismic Simulator Table. The seismic spectrum defined in EPRI TR-107330 was used as a Harsh Environment spectrum for this generic qualification in place of a plant-specific spectrum based on site survey data. 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 OBEs in succession,
- One SSE, and
- Post seismic test inspection and operability test.

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

- Accelerometers attached to representative locations on the Test Specimen,
- 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.

A preliminary resonance test was conducted to determine if the Test Specimen components has any resonant frequencies within the RRS. The test was conducted by imposing a low level sinusoidal sweep. Overall requirements for the resonance search were governed by IEEE Std 344.

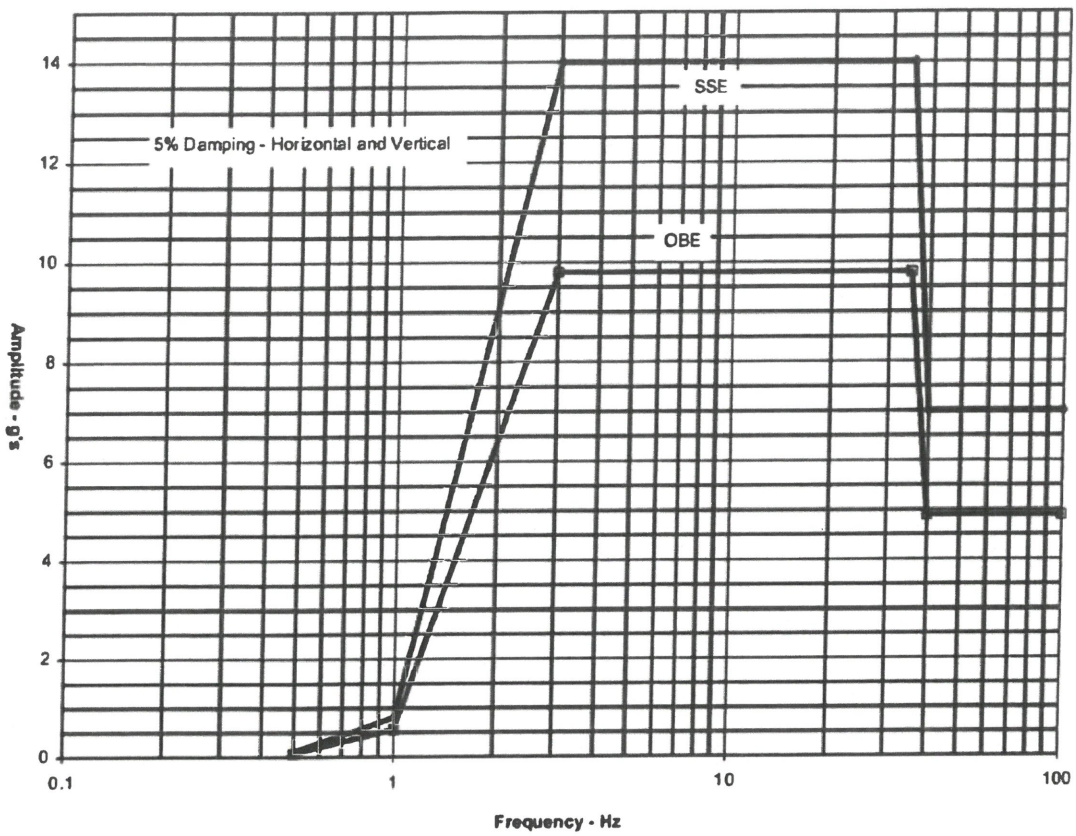

Figure 25. Seismic Test Spectrum

The total test run consists of five separate OBE RRS tests conducted in succession at 5% damping followed by one SSE RRS test conducted at 5% damping. While each dynamic test was in progress, an HFC test engineer ran the specified combination of automated tests to verify overall system performance. Following each dynamic test, the entire Test Specimen was examined for mechanical damage. Any mechanical damage sustained during testing was recorded and subsequently reported in detail in the seismic test report.

Overall acceptance were as follows:

- All connections shall remain intact, all modules shall remain fully inserted, and no functional or non-functional parts shall fall off. Tightening fasteners between successive OBEs or before the SSE does not constitute a failure condition.
- The Test Specimen shall withstand application of the SSE spectrum after application of five OBEs.
- The Test specimen shall meet its performance requirements during and following application of an SSE simultaneously applied in three orthogonal directions.
- Results of Operability and Prudency tests remain within acceptance criteria before, during, and after the seismic test runs.

The Test Specimen met all acceptance criteria during the five OBE and one SSE tests.

Detailed results of this testing are discussed in TR901-302-01, Section 10.

8.2.5 Post Qualification Tests

The Post Qualification Tests consisted of running complete Operability and Prudency tests as described in Section 8.2.2 and 8.2.3 at the HFC Facility after completion of all qualification testing. The purpose of the Post Qualification Tests was to capture performance records of the Test Specimen after being subjected to the full suite of qualification tests, and all the stress conditions therein. These test results were then compared to those from the Prequalification Test results to establish the overall change or resistance to change of the HFC-FPGA modules as caused by qualification testing. The overall acceptance criteria were identical to those performed before all equipment qualification testing. The test specimen met all acceptance criteria in post qualification testing. The test results are detailed in TR901-302-01, Section 11.

8.2.6 Test Results and Conclusion

The test results for all qualification testing consists of a description of specific test conditions, analyzed data of automated tests conducted, and a report from the testing laboratory. A final summary of test results is detailed in TR901-302-01, Section 12. EMI/RFI testing results from NTS Plano are detailed in PR037435, which is included as Attachment 13.18 of TR901-302-01. Environmental testing results from ETL Dallas are detailed in ETL Certificate of Test 13999, which is included as Attachment 13.19 of TR901-302-01. Seismic testing results from ETL Dallas are detailed in 14149 IEEE Seismic Qualification Test Report, which is included as Attachment 13.25 of TR901-302-01. The EMI/RFI, Environmental, and Seismic conditions the VV0115 Test Specimen was subjected to through the course of these tests was a generic set of harsh environmental conditions used to follow the guidance set forth in RG 1.209.

The Test Specimen was found to have operated normally during and following all qualification testing. All data logged during each Step of qualification tests was analyzed and compared to the acceptance criteria listed in Section 8.2.1-8.2.5. In-depth analysis of this data is included in TR901-302-01 for each qualification test. The Test Specimen met all the acceptance criteria listed for Prequalification Tests, Operability Tests, Prudency Tests, Environmental Stress Qualification Tests, EMI/RFI Qualification Tests, Electrostatic Discharge Tests, Surge Withstand Tests, Seismic Tests, and Post Qualification Tests.

9.0 CONCLUSION

The HFC-FPGA system platform implements the functional characteristics of the HFC-6000 system platform using FPGA hardware architecture. The design and implementation of the HFC-FPGA system platform have followed discipline specifications and development lifecycle process that meet the requirements of the 10 CFR Part 50 Appendix B and NQA-1 program as well as applicable industry standards.

The HFC-FPGA system qualification tests were constructed and performed in accordance with EPRI TR-107330, as the HFC-FPGA system is functionally the same as the microprocessor-based HFC-6000 system. Validation and Verification were performed on the HFC-FPGA system to ensure the design was complete, correct, and met the requirements for use as a safety system in NPPs.

Based on the design and implementation of the HFC-FPGA system including EQ results and V&V analysis, HFC concludes that the HFC-FPGA system, specifically the FPGA modules listed in Table 1, is qualified to be used in safety applications in NPPs. Therefore, HFC requests the NRC to amend the SE of the HFC-6000 Safety Platform to include HFC-FPGA system platform.