HF Controls

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

RR901-107-10 Rev D

Effective Date: 4 / 4 / 2018

Prepared By: Eugene O'Donnell

Reviewed By: Yin Guo

Approved By: Steve Yang

HFC

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
24/1/2016	B2	J Taylor	Remove loop controller references
5/27/2016	B	E. O'Donnell	Addition of FCPUX and FPUM2
7/10/2017	C	E. O'Donnell	Added detail from EQ results
3/8/2018	D	E. O'Donnell	Update of references for NUREG 0800-7

Table of Contents

List of Figures

List of Tables

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 (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 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. The qualification program for these modules was performed using the regulations, codes, standards and, guidance as discussed in Section 8 that are applicable to the design and qualification of digital safety systems and the scope of this amendment. This qualification program was performed to demonstrate compliance with EPRI TR-107330, and the 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. This was done in the following steps:

a) Define an architecture overview of the HFC-FPGA system and evaluate the suitability for the intended application. Input/Output modules, communication, and controller modules were defined so as to encompass a broad range of nuclear applications, in the same manner as the original HFC-6000 submittal.

b) Ensure that new HFC-6000 modules are developed using the existing and qualified HFC QA Program.

c) Select a set of modules, supporting devices and software from the HFC-6000 system to be used as the qualification test specimen and included in qualification project including the modules listed in Table 1.

d) Define and produce a Test System Application Program (TSAP). The TSAP serves as a synthetic application that is designed to aid in the qualification tests and demonstrate the acceptability of the system being qualified. This TSAP supports manual and automated testing before, during, and after equipment

qualification activity as required in EPRI TR-107330 Section 5.

e) Combine modules of the Test Specimen and the TSAP into a suitable test configuration and perform a set of acceptance tests. This activity constitutes the system integration testing for the VV0115 Test Specimen.

f) Specify the set of hardware qualification tests to be performed on the Test Specimen, including a defined set of tests to be conducted at suitable times in the qualification process.

g) Perform the hardware qualification tests, perform the data analyses, and document the results. These results and analyses are reported in TR901-302-01.

h) Ensure that the configuration identification and management program for the HFC-FPGA hardware and software is maintained using the guidelines contained in the applicable standards and regulations.

i) Ensure that all specifications of the HFC-FPGA system are consistent with the requirements of 10 CFR 50 Appendix B, IEEE Std 603-1991, the applicable GDCs, and the original HFC-6000 system. Ensure that all applicable RGs and industry standards have been followed or adequate justification provided.

The plant specific application software will be developed in accordance with the provisions of BTP HICB-14 to qualify this software on plant specific basis.

HFC requests that the NRC review the HFC–6000 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, the modules' relationship with the qualified HFC-6000 system.

2.0 REFERENCES

2.1 DEFINITIONS

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

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

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

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

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

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

Form-Fit-Function (F3) Criteria for interchangeable items with the same requirement.

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-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

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

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 AND ABBREVIATIONS

A	Ampere
AC	Alternating Current
ACE	Abnormal Conditions and Effects

ADC	Analog/Digital Converter
AI	Analog Input
ANSI	American National Standards Institute
AO	Analog Output
ASME	American society of Mechanical Engineers
ASTS	Automatic Seismic Trip System
AUX	Auxiliary
BOE	Burst of Events
BTP	Branch Technical Position
C	Celsius/Centigrade
CFR	Code of Federal Regulations
C-Link	Communication link between HFC-6000 controllers (not FPGA) implemented with a token-passing protocol
CRC	Cyclic Redundancy Check
DAC	Digital/Analog Converter
dB	Decibel
dc	Direct Current
DI	Digital Input
DO	Digital Output
DPM	Dual Ported Memory
DSP	Digital Signal Processor
EFT	Electric Fast Transient
EMI	Electro-Magnetic Interference
ELPC	Ethernet Low Pin Count Connection Interface
EPRI	Electric Power Research Institute
ESD	Electrostatic Discharge
ESFAS	Engineered Safety Features Actuation System
EWS	Engineering Workstation
F	Fahrenheit
F3	Form-Fit-Function
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
HFC	HF Controls
HICB	Instrumentation and Control Branch
HPAT	HFC Plant Automatic Tester
HPI	HFC Peripheral Interface
HSIM	High Speed Interface Module
Hz	Hertz
I&C	Instrumentation and Control
ICL	Intercommunication Link
IEC	International Electrotechnical Commission

IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
I/O	Input/Output
KHz	kilo-Hertz
kV	kiloVolt
LED	Light-Emitting Diode
mA	milli-Ampere
MCL	Master Configuration List
MFM	Master-for-a-Moment
MHz	Mega Hertz
MS	Microsoft
NC	Normally Closed
NO	Normally Open
NQA	Nuclear Quality Assurance
NRC	Nuclear Regulatory Commission
OBE	Operating Basis Event
PCB	Printed Circuit Board
QA	Quality Assurance
QAPM	Quality Assurance Program Manual
RAD	Unit of Radiation
RAM	Random Access Memory
RF	Radio Frequency
RFI	Radio Frequency Interference
RG	Regulatory Guide
RH	Relative Humidity
RIF	Redundant Interface
ROM	Read-Only Memory
RRS	Required Response Spectrum
RTD	Resistance Thermal Detector
SCM	Software Configuration Management
SE	Safety Evaluation
SER	Safety Evaluation Report
SOE	Sequence of Events
SPI	Serial Peripheral Interface
SPM	Software Program Manual
SQL	Structured Query Language
SRS	Software Requirement Specification
SSE	Safety Shutdown Event
Std	Standard
SWC	Surge Withstand Capability
TC	Thermocouple
TPM	Tri-Ported Memory
TR	Topical Report
TRS	Test Response Spectrum
TSAP	Test Specimen Application Program
VGA	Video Graphic Array
v/V	Volts
w	Watt

3.0 REGULATIONS, CODES, STANDARDS, GUIDANCE AND REFERENCES

3.1 NRC REGULATIONS AND GUIDANCE, INDUSTRY STANDARDS, AND HFC 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.

3.1.1 NRC Regulations and Guidance

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"
10 CFR Part 50.34	"Contents of Applications; Technical Information"
10 CFR Part 50.36	"Technical Specifications"
10 CFR Part 50.49	"Environmental Qualification of Electric Equipment Important To Safety for Nuclear Power Plants"
10 CFR Part 50.54	"Conditions of Licenses"
10 CFR Part 50.55	"Conditions of Construction Permits, Early Site Permits, Combined Licenses, and Manufacturing Licenses"
10 CFR Part 50.59	"Changes, Tests and Experiments"
10 CFR Part 52.47	"Contents of Application; Technical Information"
10 CFR Part 52.80	"Contents of Applications; Additional Technical Information"
NUREG-CR-6303	"Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems"
NUREG-0737	"Requirements for Emergency Response Capability"
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

Regulatory Guide

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

RG 1.28 "Quality Assurance Program Criteria", 2010

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 1.70	"Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants", 1978
RG 1.75	"Independence of Electrical Safety Systems", 2005
RG 1.89	"Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants", 1984
RG 1.97	"Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants", 2006
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 1.151	"Instrument Sensing Lines", 2010
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 1.174	"An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant Specific Changes to the Licensing Basis", 2011
RG 1.177	"An Approach for Plant-Specific Risk-Informed Decision Making: Technical Specifications", 2011
RG 1.180	"Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems", 2003
RG 1.189	"Fire Protection for Operating Nuclear Power Plants", 2009
RG 1.200	"An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities", 2009
RG 1.204	"Guidelines For Lightning Protection Of Nuclear Power Plants", 2011

RG 1.206 "Combined License Applications for Nuclear Power Plants (LWR Edition)", 2007

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

RG 5.71 "Cyber Security Programs for Nuclear Facilities", January 2010

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"

3.1.2 Industry Standards

ASME NQA-1/NQA-1a	"Quality Assurance Requirements for Nuclear Facility Applications", 2008/2009
EPRI TR-102323	"Guidelines for Electromagnetic Interference Testing of Power Plant Equipment", Rev.2 November 2000
EPRI TR-107330	"Generic Requirements Specifications for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants", December 1996
IEC 61000-4-2	"Electrostatic Discharge 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 61000-4-6	"Immunity to Conducted Disturbances", Edition 3, 2008
IEC 61000-4-12	"Oscillatory Waves Immunity Test", Edition 2, 2006
IEEE Std C37.90.1	"IEEE Standard Surge Withstand Capability (SWC) Tests for Protective Relays and Relay Systems (ANSI)", 1989
IEEE Std C62.41	"Recommendation Practice on Surge Voltage in Low-Voltage AC Power Circuits", 1991
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 Electric Equipment for Nuclear Power Generating Stations", 1987
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 577	"IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Power Generating Stations", 1976
IEEE Std 603	"IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations", 1991
IEEE Std 730	"IEEE Standard Software Quality Assurance Plans", 1989
IEEE Std 828	"IEEE Standard for Software Configuration Management Plans", 1990
IEEE Std 829	"IEEE Standard for Software Test Documentation", 2008
IEEE Std 830	"IEEE Standard Guide for Software Requirements Spec.", 1998
IEEE Std 1008	"IEEE Standard for Software Unit Testing", 1987
IEEE Std 1012	"IEEE Standard for Software Verification and Validation", 2004
IEEE Std 1016	"IEEE Recommended Practice for Software Design Description", 2009
IEEE Std 1028	"IEEE Standard for Software Reviews and Audits", 2008
IEEE Std 1042	"IEEE Guide to Software Configuration Management", 1987
IEEE Std 1074	"IEEE Standard for Developing Software Life Cycle Processes", 2006
IEEE Std 1228	"IEEE Standard for Software Safety Plans", 1994
MIL-STD-461E	"Measurement of Electromagnetic Interference Characteristics"

3.1.3 HFC Technical Documents

DS001-007-01	HFC-FPGA Module System Component Design Description
DS001-007-02	HFC-6000 FPGA System IP Core Design Description
DS001-007-03	FPGA Controller Logic Library Component Design Description
DS001-007-04	HFC-FCPU FPGA Software Design Description
DS002-000-01	C-Link Protocol Design Specification
DS901-001-54	HFC-FPUD Hardware 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
DS901-002-18	HFC-FCPUX Hardware Design Specification
DS901-002-19	HFC-FPUM2 Hardware Design Specification
DS901-003-01	HFC-FPUD Software Design Specification
DS901-003-02	HFC-FPUA Software Design Specification
DS901-003-03	HFC-FPUL Software Design Specification
DS901-003-04	HFC-FPUAO Software Design Specification
DS901-003-05	HFC-FPUM Software Design Specification
MS901-000-08	HFC-FPGA System Design Specification
PP901-000-01	HFC-6000 System Topical Report
QAPM	HFC Quality Assurance Program Manual
RR901-000-23	HFC-6000 Security Concept
RR901-107-01	FMEA for HFC-6000 FPGA Controllers
RR901-107-02	Reliability and Availability Analysis Report for FPGA Controllers
RR901-107-03	EPRI TR 107330 Requirements Compliance Traceability Matrix for HFC-6000 FPGA Modules
TP901-115-01	VV0115 Qualification Operability Test Procedure
TP901-115-02	VV0115 Qualification Prudency Test Procedure
TP901-115-05	VV0115 Integration Test Plan
TP901-115-06	VV0115 TSAP Validation Test Procedure
TP901-200-01	EPRI TR 107330 Burn-in Test Procedures
TP901-302-02	VV0115 Environmental Stress Test Procedure
TP901-302-03	VV0115 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 Seismic Test Procedure
TR901-302-01	HFC-FPGA Control System of HFC-6000 Safety Platform Qualification Test Report
VV901-300-09	VV0115 Qualification Master Test Plan
VV901-300-10	HFC-6000 FPGA Test Specimen Design Description

3.1.4 HFC-6000 NRC Reviewed Documents

ML080780170 HFC-6000 Safety System Topical Report

ML100820253 HFC-6000 Radiation Exposure Evaluation

ML110831014 NRC Safety Evaluation Report of HFC-6000 Safety Platform

ML111990323 ERD111 Qualification Retest Summary Report

ML11297A039 to 042 Amendment for the Enhanced Equipment of HFC-6000 Safety Evaluation Report (with Supporting Documents)

3.1.5 HFC Quality Procedures

HFC Software Program Manual

Quality Assurance Program Manual

QPP 3.1 Design Control

QPP 3.2 Product Development Lifecycle and Verification & Validation Program

4.0 HFC-FPGA SYSTEM OVERVIEW

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 HSIM F-Link module, and Gateway module as listed in Table 1. The individual modules communicate with one another via RS-485 traces on the backplane of the HFC-6000 rack using the token-passing protocol originally developed for the C-Link. However, these modules have no hardware interface with the C-Link and so require a Communication Gateway controller to broadcast their status to the overall control system. As with the qualified modules from the HFC-6000 system, all modules in the HFC-FPGA system only communicate with plant equipment via I/O interfaces.

In order to support development of the present amendment to the NRC SE-approved HFC-6000 safety platform, a test specimen was created from the HFC-FPGA I/O and controller modules. This test specimen consisted of two expansion racks with one or more of each of the modules listed in Table 1. Additional equipment was included to supply operating power and communication connectivity. This equipment is not listed either due to having been previously qualified or being excluded from the scope of the present amendment, and is detailed in the document VV901-300-100, HFC-6000 FPGA Test Specimen Design Description. This test specimen was then tested based on EPRI TR 107330 in accordance with the overall test program described in HFC-6000 NRC Topical Report. Figure 1 illustrates the overall arrangement for testing. Modules for qualification addressed in this amendment are located in the labelled green box in Figure 1. To ensure the HFC-FPGA modules qualify in the same way as previous HFC-6000 assemblies, operability and prudency tests were developed based on the requirements in EPRI TR 107330 Section 5 to test the full test specimen. Data collected from different hardware configurations were compared and analyzed to verify that the new hardware designs are

at least equivalent in performance and reliability to the original HFC-6000 test specimen for each test category.

[

]

Figure 1. Test Specimen Equipment Block Diagrams

Table 1. Qualification Modules

Part Number	Module Name	Description
40117421Q	HFC-FPUD01	FPU I/O Module for 16 DI Channels and 16 DO Channels
40117422Q	HFC-FPUD02	FPU I/O Module for 32 DI Channels
40124221Q	HFC-FPUA01	FPU I/O Module for 16 4- to 20-mA AI Channels
40129421Q	HFC-FPUAO	FPU I/O Module for 8 4- to 20-mA AO Channels
40127021Q	HFC-FPUL	FPU I/O Module for 8 AI Channels for Type E Thermocouples
40127421Q	HFC-FPUM	FPU I/O Module for 8 AI Channels for 100-Ohm Platinum RTDs
40145621Q	HFC-FPUM2	FPU I/O Module for 8 AI Channels for 100-Ohm Platinum RTDs
40132221Q	HFC-FCPU	CPU for the FPU Controller product line
40145221Q	HFC-FCPUX	CPU for the FPU Controller product line
40108621Q	HFC-HSIM	F-Link High Speed Interface Module
40103834Q	HFC-FPC08	Communication Gateway Controller Without VGA

4.1 SYSTEM COMPONENTS

Table 1 indicates the different modules covered by the present amendment. The FPUD module has two versions that differ only in the characteristics of the hardware I/O interface. The FCPU and FCPUX controller modules are comprised of different hardware but are identical in function and operation within the scope of this amendment as centralized controller modules. The FPUM and FPUM2 modules are comprised of different hardware but are directly interchangeable in pinout, function, and operation as RTD input modules. All of the HFC-FPGA module designs are based on two FPGA modules – a Control FPGA and a Diagnostic FPGA. The Control FPGA contains program code that controls every functional process controlled by the module. The Diagnostic FPGA contains program code that operates in synchronized operation with the Control FPGA that serves to validate both the process operation and the results of that operation. In HFC Documentation, “Process FPGA” and “Control FPGA” are synonymous and may be used interchangeably. A summary of the processes to be tested and validated are summarized below:

- Hardware/software initialization verifies that the module is fully operational and ready for online operation. Any failure of initialization testing will prevent the module from starting normal online operation.

- F-Link Communication. All modules installed in the same rack are configured as nodes on a common F-Link. The remote number and link sequence number are hard-coded to the backplane connector of each I/O slot, so the module position in the rack determines its identity on the link. All communication errors are logged

and broadcast as part of module status. In addition, the Diagnostic FPGA validates every broadcast packet before it is broadcast; and if a fault is detected, it will block broadcast of the packet to the link.

- I/O Interface. Each module type has its unique hardware interface with the field equipment. The Control FPGA initiates the scan process, but the Diagnostic FPGA receives the same control signals and monitors them. The I/O interface must receive both the control signals from the Control FPGA and the correct monitored signals from the Diagnostic FPGA for the process to proceed. Both the Control and Diagnostic FPGAs receive the same input data via different hardware routing, so they exchange their images to enable data validation. Any failure results in rejection of the data input and an error indication.

- Control FPGAs for AI modules execute regularly scheduled calibration cycles. Detection of component drift will result in calculation of correction factors on a channel-by-channel basis. However, if the magnitude of the deviation exceeds a programmed tolerance, then the module will log an error and enter a failure state requiring module replacement.

- Redundant Controller Interface (RIF) Communication. The HFC-FCPU is normally implemented as a redundant controller set and installed in adjacent card slots. If operational, the HFC-FCPU installed in the even slot takes the role of primary controller, and the module in the odd slot is secondary. The RIF is a dedicated serial communication link between the two HFC-FCPU modules that enables status drops from primary to secondary. The HFC-FCPUX is implemented using the same RIF as the HFC-FCPU.

- G-Link Communication. There is no direct communication between the HFC-FPGA controllers and the C-Link, which serves as the common data highway for an HFC-6000 control system. Instead, an HFC Gateway module is connected to the C-Link, and a dedicated G-Link is connected to the redundant HFC-FCPU and HFC-FCPUX modules. The Gateway module manages communication with the C-Link, and the redundant HFC-FCPU/HFC-FCPUX modules control status transfer to the Gateway.

4.2 VERFICATIONS AND VALIDATIONS

All HFC product development lifecycles are conducted in accordance with HFC quality process procedures which are NQA-1 2008 compliance. In addition, HFC design control process procedure is conducted in accordance with IEEE 1012-2012 which includes both hardware V&V and software V&V. The software V&V process of IEEE 1012-2012 is compatible with the IEEE 1012-2004 revision.

4.3 EQUIPMENT QUALIFICATION

The complete set of qualification tests mandated by EPRI TR 107330 and NRC RG 1.180 cover the following:

a) Application Object Tests,
b) Test Specimen Pre-Test,
c) Environmental Stress Tests,
d) Seismic Stress Test,
e) EMI/RFI Tests,
f) Electrostatic Discharge Tests,
g) Surge Withstand/EFT/Burst Immunity Tests, and
h) Test Specimen Post Test.

Test results demonstrate overall functional capabilities of each module included in the test program. Refer to TR901-302-01 for detailed coverage of the test program and test results for each module.

5.0 HFC-FPGA CONTROL SYSTEM HARDWARE/SOFTWARE

All of the HFC-FPGA modules covered by this amendment share similar hardware and software architecture. 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)
- 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 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.

5.1 HARDWARE ARCHITECTURE

5.1.1 Common Kernel

The hardware designs for all HFC-FPGA module assemblies include the following components:

- Two FPGA modules that communicate with one another via an HFC Peripheral Interface (HPI) link. The Control and Diagnostic FPGAs are identical hardware components but have different functional roles in the assembly.

- 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. And 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.

- PCB ID interface enables the FPGAs to read the module ID from the hardwired code on the backplane.

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

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

- Board-edge LEDs provide a visual indication of PCB operating status for communication and error codes.

5.1.2 Module-Specific Components

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 design specification for each board type for detailed information on the I/O interface designs.

5.1.2.1 HFC-FPUD01/02

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 HFC-FPUA

The HFC-FPUA Module is an analog input module designed to support 16 AI channels. Within the scope of this amendment, only the HFC-FPUA01 version is to be considered for qualification. The HFC-FPUA01 supports 16 AI channels in the

range of 4-20 mA.

5.1.2.3 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.

5.1.2.4 HFC-FPUL

The HFC-FPUL Module is an analog input module designed to support 8 TC AI channels. These 8 TC AI channels operate to receive signals from Type E thermocouples.

5.1.2.5 HFC-FPUM

The HFC-FPUM Module is a precision RTD-measuring module designed to support 8 RTD input channels. These 8 RTD input channels support four ranges: Low (0-50 °C), Medium (0-100 °C), Wide (0-200 °C), and a 0-2000 Ω range. These ranges are selected by changing the configuration of onboard switches.

5.1.2.6 HFC-FPUM2

The HFC-FPUM2 Module is a precision RTD-measuring module designed to support 8 RTD input channels. These 8 RTD input channels support four ranges: Low (0-50 °C), Medium (0-100 °C), Wide (0-200 °C), and a 0-2000 Ω range. These ranges are selected by changing the configuration of onboard switches. This module is similar in function as the FPUM, but has a different layout and is designed to have a higher input accuracy.

5.1.2.7 HFC-FCPU

The HFC-FCPU Module is a central control unit designed for use in the HFC-FPGA system. This module supports communication between I/O modules (F-Link), the Gateway Controller (G-Link), and a redundant HFC-FCPU (RIF). The HFC-FCPU module also supports 8 DO channels, but I/O functionality was not included in the scope of this amendment for this module.

5.1.2.8 HFC-FCPUX

The HFC-FCPUX Module is a central control unit designed for use in the HFC-FPGA system. This module supports communication between I/O modules (F-Link), the Gateway Controller (G-Link), and a redundant HFC-FCPU (RIF). The HFC-FCPUX module is similar in function to the HFC-FCPU, but has a different layout and is designed to support a larger capacity FPGA chip.

5.1.2.9 HFC-HSIM

The HFC-HSIM Module is an information carrier for the HFC-6000 system. This

module supports the transmitting and receiving of serial data from an ICL or F-Link bus, and communicates this information over a fiber optic line to a second HSIM module. Within the scope of this amendment, only the F-Link data transfer functionality is to be considered.

5.1.2.10 HFC-FPC08

The HFC-FPC08 Gateway Module is a gateway communication device that facilitates communication between outside equipment and the centralized controllers. This module supports 2 Ethernet ports that 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.

5.1.3 Power Distribution and Chassis

All power sources for HFC-6000 control systems are external to the controller hardware. 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-6000 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. 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-6000 backplane, and these power traces are isolated from everything else on the assembly. 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.

5.1.4 Communication Links

All previous implementations of HFC-6000 control systems included two different hardware arrangements for communication:

- ICL: Redundant RS-485 traces from the controller to each I/O slot. A redundant remote controller served as the one link master, and it initiated communication with each configured I/O module by means of a Poll-Response protocol. The Poll-Response protocol ensured deterministic

operation by imposing fixed time limits for each phase of the exchanges.

- C-Link: Redundant Ethernet links connecting all remotes making up a control system. This link uses a token-passing protocol enabling each remote configured on the link to take mastership for a limited period of time. While a particular remote is master, it can broadcast all of its accumulated status to the link. All other remotes on the link receive these broadcasts and use the data as needed. After the mastership interval expires for a particular remote, the current master relinquishes mastership to the next remote in sequence. This protocol ensures deterministic operation by imposing a fixed limit on the mastership time slot for each remote.

The I/O modules covered by this document 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 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 HSIM module. Figure 2 illustrates the communication arrangement for each configured module installed in the rack.

[

]

Figure 2. F-Link Arrangement

Each HFC-FPGA I/O module and HFC-FCPU/FCPUX controller includes redundant onboard RS-485 transceivers designated as F-Link channel 0 and channel 1. Because this 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 developed for the F-Link. Refer to DS002-000-01 for detailed information about the C-Link protocol. 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 slot number, which is hard wired to each I/O slot in the PCB rack. Consequently, the HFC-FPGA I/O module in slot 0 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 module I/O relinquishes the token, mastership passes back to Station Address 0. The HSIM module allows for the passing of F-Link information between remotes via fiber optic lines.

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 FCPU/FCPUX controllers. This link enables the primary FCPU/FCPUX to transfer current status images to the secondary FCPU/FCPUX throughout normal controller operation.

Similarly, the G-Link is a dedicated communication path between the redundant FCPU/FCPUX controllers and the Gateway Controller module. This link enables transfer of overall control status from the FCPU/FCPUX to the common C-Link data highway. In the scope of this amendment, the Gateway Controller is the HFC-FPC08.

5.2 SOFTWARE ARCHITECTURE

The software that will be utilized for the safety related applications of the HFC-FPGA system is divided into two categories: Operating Software and Application Software. Application software is plant-specific, therefore only Operating Software will be discussed within the scope of this amendment.

Every HFC-FPGA module PCB includes two FPGAs: The Control FPGA and the Diagnostic FPGA. Figure 3 illustrates the general arrangement of both 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 are 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.

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.

[

]

Figure 3. General Arrangement of FPGA Controllers

5.2.1 Control FPGA Software for HFC-FPGA Controllers

The software for the Control FPGA is composed of several sets of software modules each of which performs a distinct function within the controllers. 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 identifies 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. For detailed information about the common library modules, refer to DS001-007-01.

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; the remainder 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 software design specification 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. Refer to DS001-007-04 for additional information.

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 CPU modules to transfer current status for the process under control to the Communication Gateway module. Refer to DS001-007-04 for additional information.

Application Processing and Support Modules. The application code for HFC-6000 control systems consists of a binary flash memory file, database, a collection of utility files, and an application logic verilog module. The binary file and application logic verilog module 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 FSM performs the block operations identified in the flash binary file with the application logic verilog module during normal operation of the control system. Refer to DS001-007-03 for the library of application-related modules supported by the present implementation of the HFC-FPGA system.

5.2.2 Diagnostic FPGA Software

The Diagnostic FPGA software controls diagnostic functions for each process controlled by the Control FPGA. 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 a scan image. This scan image 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 data images to verify that both received the same data via F-Link. If there is any discrepancy between the two, then the data is rejected as invalid. Refer to the software design specification for individual HFC-FPGA modules for more detailed information about specific software modules and functions performed by the Diagnostic FPGA Software.

5.3 APPLICATION CONTROL

In previous implementations of the HFC-6000 centralized control system, an application program resides in a single remote. The remote 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 FPGA implementation of the HFC-6000 control 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 code. 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 image 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 images are the same, distributes

the updated output images to output modules via the F-Link. The output modules verify output data, execute their function, 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.

5.4 OPERATING HISTORY EVALUATION

The HFC development and change process is strictly controlled and its integration into hardware and software is thoroughly tested. HFC quality assurance programs were applied during the development of the HFC FPFA control system of HFC-6000 platform. The HFC FPGA control system has been developed from its microprocessor-based HFC-6000 platform and therefore is viewed as part and extension of the HFC-6000 platform with the adoption of the FPGA technology. In this HFC FPGA control system, there are previously developed hardware and software components that are used in the HFC-6000 platform as described in HFC-6000 SER as well as HFC TUV SIL 3 certified controller HFC-FPC08. The hardware and software components provide necessary credits (especially for software as discussed in EPRI TR-106439) and confidence for the HFC FPGA control system to be evaluated.

The hardware and software components utilized in the HFC-FPGA control systems of the HFC-6000 platform safety applications were identified and the related operating history was evaluated. The evaluation of the operating history demonstrated that the hardware and software have significant experience in critical application, including Korean nuclear power plants. The identified hardware and software have been reliable for a long period of time, supporting the conclusion that the inherent quality makes the hardware and software suitable for dedication for use in nuclear safety applications. Furthermore, it was concluded that the operating conditions in Korean plants were either similar to or even identical to the operating conditions that will be seen in US nuclear plants.

The following are some important hardware and software components (or modules) that have been adopted for use in the HFC FPGA control system:

[

]

Additionally, One-Step tool used for HFC-FPGA applications has been adapted 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 EWS offline PC workstation in the field. The end programming file created by One-Step is employed to (re)configure the FPGA. The resulting file is finally transferred to the FPGA via a serial interface (JTAG) under a secured and documented process.

6.0 SAFETY SYSTEM DESIGN TOPICS

A nuclear power plant safety system that utilizes the HFC-6000 product line must provide deterministic performance with predictable operation and defined maximum response time characteristics. This 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, and
- RIF.

6.1 CENTRALIZED CONTROLLER MODULE CHARACTERISTICS

[

]

[

]

[

]

Figure 4. HFC-FCPU/HFC-FCPUX Block Diagram

6.2 I/O MODULE CHARACTERISTICS

[

]

[

]

[

]

Figure 5. 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 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. Specifics on the diagnostic functions of the HFC-FPGA System can be found in DS901-001-81. The diagnostic FPGA may reset the control FPGA if errors are detected.

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. This function is described in

PP901-000-01, section 8.1.5. 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-6000 system to communicate with each other. The F-Link structure is based on the token-passing protocol previously developed for the HFC Proprietary C-Link. The F-Link 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 the same token-passing protocol and message packet structure used by C-Link and defined in DS002-000-01 Appendix 1: F-Link. Further details of F-Link development and structure are defined in DS001-007-01.

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 only four exceptions:

- No address checking is performed, as the HFC-FPC08 gateway controllers are not assigned a station ID for F-Link communication.
- No I/O modules communicate using G-Link
- Communication is transmitted over a separate (from F-Link) set of redundant backplane traces.
- No ACK tokens are used, only Pass tokens

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. Output modules are provided information 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.

6.8 QUALITY ASSURANCE PROGRAM

The HFC Quality Program used for the development of the HFC-FPGA system is the same program used for the development of the HFC-6000 system from the original qualification submittal. This is detailed in PP901-000-01 Section 8.4. This program complies with

- ANSI/ASME NQA-1&1a- "Quality Assurance Requirements for Nuclear

2008/2009	Facilities"
• 10 CFR 50 Appendix B	"Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants"
• ANSI/ISO/ASQ Q9001-2000	"Quality Management Systems - Requirements"

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

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

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

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

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

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

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-6000 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-6000 product met the highest standards of technical quality.

To assure that the QA Program was being rigorously adhered to the Programs mandated; an independent verification effort to assess compliance with the QA Program and to provide ongoing assessment of the adequacy of the measures was undertaken to ensure technical correctness of the QA processes. Periodic audits of the QA Program are conducted as well.

The HFC QA program undergoes updates periodically to ensure compliance with the most recently endorsed versions of quality standards and regulations.

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

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 system to verify its ability to perform protective initiation functions. The HFC system allows complete testing of its actuated devices in accordance with the RG. This testing can be done with the plant at power or shutdown. An additional level of HFC-6000 testing is provided by diagnostic testing and onboard diagnostic FPGAs.

RG 1.28 2010 "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.

RG 1.29 2007 "Seismic Design Classification"

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 OBE and SSE seismic stress tests, at levels specified in EPRI TR-107330. This is discussed in detail in the EQ Test Report TR901-302-01.

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

As with the previously qualified modules in the HFC-6000 system, the HFC-FPGA modules covered in this amendment will be evaluated for bypass and inoperable status information on a plant-specific basis.

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

Single failures of the HFC-FPGA system have been evaluated in the report RR901-107-01. That assessment led to the conclusion that the system will meet the single failure criterion of IEEE-603 upon a plant specific implementation in a redundant safety system.

RG 1.62 2010 "Manual Initiation of Protective Actions"

All HFC-FPGA modules have the capability of initiating actuations manually, as they can be set via the EWS. Plant-specific evaluations shall be made of the system to verify this functionality at a system level.

RG 1.70 1978 "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants"

Safety Analyses on individual modules are conducted as prescribed by IEEE 1012. Safety analyses on the system level will be conducted on a plant specific basis.

RG 1.75 2005 "Independence of Electrical Safety Systems"

The design of the original HFC-6000 system addressed in PP901-00-01 conforms to this RG. 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. 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 1.89 1984 "Qualification for Class 1E Equipment for Nuclear Power Plants"

The HFC-FPGA system has been tested to verify its conformance with this RG, RG 1.209, and IEEE Std 323. The environmental qualification tests employed both type-testing and analysis which were followed per the provisions of EPRI TR-107330, and the details are described in TR901-302-01 Section 6.

RG 1.97 2006 "Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants"

The HFC-FPGA modules provide the flexibility and processing capability to accommodate a wide range of both analog and digital user instrumentation, including different voltages, analog input types, and ranges. The particular combination of instrumentation and controls that will be needed to detect and respond effectively to an accident condition will depend on the specific safety system being implemented, and will therefore be addressed on a project-by project basis.

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

The HFC-FPGA system was tested to the seismic specifications listed in EPRI TR-107330, as detailed in TR901-302-01, Section 10.

RG 1.105 1999 "Setpoints for Safety-Related Instrumentation"

HFC-FPGA modules have accuracy values in their associated Design Specifications. 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 following features built into system hardware and software for direct verification of field equipment:

- Logic detection of open AI/AO channels,
- Logic detection of out-of-range AI.

Additional utilities for periodic testing will be implemented and evaluated as part of a specific application on a project-by project basis.

RG 1.151 2010 "Instrument Sensing Lines"

The HFC-FPGA system interfaces with plant instruments via field wiring. The field wiring and interface with instrumentation will be evaluated on a plant specific 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 identical in function and design methodology to those developed for the qualified HFC-6000 system and modules. This is addressed in Sections 8.5 and 10 of PP901-00-01. FPGA-specific cyber security has been implemented for the HFC-FPGA system as addressed in RR901-000-23.

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. NUREG-0800 references this RG as necessary acceptance criteria. 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 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 identical to that used for software in the qualified HFC-6000 system and modules. Anomaly reporting

within V&V process for the HFC-FPGA system was performed per IEEE 1028

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-6000 platform's software including both the pre-developed and new software. This plan was formulated based upon the guidance provided by IEEE Std 828 and 1042 for the qualification of the HFC-6000 system, and has been used for the development and maintenance of the HFC-FPGA modules. The HFC-6000 SCM is designed to be extended to plant-specific applications as well.

RG1.170 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 and calibration information,
- Acceptance criteria, and
- Reports containing input listing, output list, test data, error logs, and conformance to acceptance criteria.

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. 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 are generated to cover specific requirements listed in the SRS for software modules, and test plans and procedures are 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.

RG 1.172 2013 "Software Requirement Specifications For Digital Computer Software And Complex Electronics Used In Safety Systems Of Nuclear Power Plants"

Software requirement specifications for the HFC-FPGA system are written to comply with and reviewed against the guidance in this RG, as well as the associated sections of IEEE 830 and IEEE 1074. 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 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. Cyber security defenses were addressed in the development cycle as described in RR901-000-23, and software safety analyses were performed per IEEE 1012.

RG 1.174 2011 "An Approach For Using Probabilistic Risk Assessment In Risk-Informed Decisions On Plant Specific Changes To The Licensing Basis"

Compliance with RG 1.174 will be assessed on a plant specific basis and is not considered within the scope of this platform-level topical report.

RG 1.177 2011 "An Approach For Plant-Specific, Risk-Informed Decision Making: Technical Specifications"

Compliance with RG 1.177 will be assessed on a plant specific basis and is not considered within the scope of this platform-level topical report.

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, and the results are detailed in TR901-302-01, Section 7.

RG 1.189 2009 "Fire Protection for Nuclear Power Plants"

Use of the HFC-FPGA system in any fire protection systems will be evaluated on a plant specific basis.

RG 1.200 2009 "An Approach For Determining The Technical Adequacy Of Probabilistic Risk Assessment Results For Risk-Informed Activities"

Probabilistic risk assessment and subsequent related activities will be conducted on a plant specific basis

RG 1.204 20011 "Lightning Protection of Nuclear Power Plants"

Compliance with the RG is dependent on specific plant application, and is therefore outside of the scope of this amendment,

RG 1.206 2007 "Combined License Applications for Nuclear Power Plants"

HFC has reviewed this RG and noted the guidance and requirements standards that are applicable for the qualification of a safety related digital platform. The plant-specific items addressed by this RG report will be evaluated during plant-specific implementations.

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 TR901-302-01, Section 6.

RG 5.71 2010 "Cyber Security Programs For Nuclear Facilities"

The HFC-FPGA system has been designed in compliance with RG 1.168, and the incorporation of the HFC-FPGA platform into a plant's overall Cyber Security program will be evaluated on a plant-specific basis.

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 7.10 of this report. Details regarding this concept will be provided during plant specific implementations.

NUREG-0737 "Requirements for Emergency Response Capability"

The HFC-FPGA system will follow the guidance provided by this NUREG for any plant-specific implementation.

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

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

The HFC-FPGA modules are designed for in-service testability of hardware and software components. Per the previously described FMEA RR901-107-01, HFC surveillance testing and automatic self- testing measures provide adequate mechanisms to detect certain failures.

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 comply with GDC 21, as well as RG 1.152 and IEEE 7-4.3.2. Purchased PLC hardware, embedded and operating systems software, tools, and peripheral components are tested and evaluated to a level commensurate with the system they are designed to support. All changes to these items are controlled under the configuration management system described in the QAPM. 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 7.10. 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. 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"

The HFC-FPGA modules were developed using the same design program as described in PP901-000-01, section 8.5.3. This includes software development in compliance with IEEE Std 7-4.3.2. The quality plan used is consistent with ASME NQA-1a, and addresses all runtime resident software. The pre-developed software is qualified based on the provisions of Section 5.3.2 and Appendix D of the IEEE Std. Qualification factors were developed per the guidance of EPRI's TR-106439 and TR-107330. Specific compliance with sections of TR-107330 is detailed in RR901-107-03.

Software Qualification was performed in environments that are representative of those used in installed HFC-FPGA systems, for all software, process, and diagnostic FPGAs. This includes exercising and monitoring memory, processors, inputs and outputs, diagnostics, associated components, communication paths, and interfaces. Testing demonstrated that the performance requirements related to safety functions were met. Failure modes were tested to have consistent behavior for failure to the intended state, and will be evaluated on a plant-specific basis.

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

The HFC-FPGA system and module-level requirements were generated to be in compliance with IEEE Std 279. Furthermore, Section 4 of this IEEE Std are covered in great detail by the compliance with EPRI TR-107330.

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

The HFC-FPGA modules were environmentally qualified as detailed in Section 5 of TR901-302-01.

IEEE Std 344-1987 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 10 of TR901-302-01.

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 is detailed in RR901-107-02. These

results show that this system is highly reliable and acceptable for use in safety related systems. The results of the FMEA are detailed in RR901-107-01, and show that the HFC-FPGA modules meet the acceptance criteria. A plant-specific analysis of FMEA and reliability will be conducted for specific plant applications.

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 meets the single failure requirements in this IEEE standard as well as IEEE 603, and will be evaluated at a plant specific implementation level.

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

The review to meet the guidance of the IEEE Std should occur during the plant-specific implementation phase. 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. Independence of the C-Link interfaces remains unchanged from that discussed in PP901-000-01, Section 8.9.

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

As discussed in the response for IEEE Std 352, see RR901-107-02 for Reliability and Availability results.

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. These requirements as well as those detailed in EPRI TR-107330 have been taken into account for all modules of the HFC-FPGA system design.

IEEE Std 730-1989 "IEEE Standard for Software Quality Assurance Plans"

The HFC-FPGA modules were designed under the same quality assurance plan used to develop the qualified HFC-6000 system, detailed in PP901-000-01 Section 8. This software quality assurance plan is compliant with this IEEE Std as well as 10 CFR Part 50, Appendix B.

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 the response to NRC RG 1.169 in section 6.9.2 of this

report.

IEEE Std 829-2008 "IEEE Standard for Software 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 Standard Guide for Software Requirements Specification"

Software requirement specification guidance is discussed for 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.

IEEE Std 1012-2004/2012 "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.

IEEE Std 1016-2009 "IEEE Recommended Practice for Software Design Description"

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 are written to be highly readable and viewable with clear descriptions of component software purposes and attributes.

IEEE Std 1028-2008 "IEEE Standard for Software Reviews and Audits"

The Quality Assurance Program for the HFC-6000 system complies with this IEEE Std, and assures that the requisite software reviews and audits are performed. This Quality Assurance Program remains in place for the development of the HFC-FPGA modules addressed in this amendment.

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

The Software Configuration Management program for the HFC-6000 is discussed in PP901-000-01, Section 10 and also addressed in the RG 1.169 discussion above. This program remains unchanged from the HFC-FPGA system.

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 software for the HFC-6000 system, including all application software. See the RG 1.173 discussion in Section 6.9.2 of this report, as well as Section 10 of PP901-000-01. 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.

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

The HFC-6000 system design includes the aspects of software safety management, software safety analyses, and post development which include training, installation, startup and transition, operations support, monitoring maintenance, and retirement. The HFC-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.

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

Surge Withstand capability was conducted per USNRC RG 1.180, and the details are discussed in TR901-302-01, Section 9.3.

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 TR901-302-01, Section 7.

ASME NQA-1/NQA-1a "QA of Design Software"

The HFC quality assurance processes follow the guidance presented in these ASME standards and also meet the requirements of 10 CFR 50 Appendix B. PP901-000-01 Section 8 provides a summary of the quality assurance process for the HFC-6000 system. The HFC-FPGA modules were developed under the same base QA processes that have been updated to meet the changes in NQA-1/NQA-1a as they are accepted by the USNRC.

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

Compliance of the HFC-FPGA modules with this EPRI TR is detailed by section in RR901-107-03.

6.9.5 CFR and General Design Criteria

a) GDC 1 – Quality Standards and Records

The HFC-6000 QA procedures and record-keeping both conform to this requirement. The HFC-FPGA modules were designed under the QA procedures listed in the HFC QAPM.

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 are in conformance with this requirement

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. The results of this testing show that the HFC-FPGA modules are in conformance with this requirement

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 are designed and tested to this requirement across ranges anticipated for plant installations in general, as outlined in EPRI TR-107330.

f) GDC 19 – Control Room

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

g) GDC 20 - Protection System Functions

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

h) GDC 21- Protection System Reliability And Testability

Testability of the HFC-FPGA modules is a main design criteria, and is verified

throughout the design process. The reliability of HFC-FPGA modules has been calculated and is detailed in RR901-107-02.

i) GDC 22 - Protection System Independence

Protection system independence for the HFC-6000 based safety systems meets 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 PP901-000-01 Section 8.9. Plant specific implementation will provide a plant-wide system level independence design that should 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 TR901-302-01.

k) GDC 24 - Separation of Protection and Control Systems

The HFC-6000 system including HFC-FPGA modules 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.

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

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

m) GDC 29 - Protection Against Anticipated Operational Occurrences

HFC-FPGA based protection and reactivity control systems will continue to meet the requirements of this GDC. Details are to be part of the plant specific implementation review.

n) GDC 37 - Testing of Emergency Core Cooling System

The ESFAS HFC-6000 system applications will support this requirement with its configurations for periodic and functional testing, and can be supported using the HFC-FPGA modules. However, details are 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, 48-53, 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 50.34 "Contents Of Applications; Technical Information"
Platform-level safety analyses have been performed for the HFC-FPGA system as listed in RR901-107-03 EPRI TR 107330 Requirements Compliance Traceability Matrix for HFC-6000 FPGA Modules. This will allow for plant-specific safety evaluations and comparisons when needed for plant-specific applications.

10 CFR 50.36 "Technical Specifications"

The Design Specifications listed in Section 3.1.3 of this report are the technical specifications for each module in the HFC-FPGA platform. Technical specifications for the system and application logic will be generated and assessed on a plant-specific basis.

10 CFR 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 TR901-302-01.

10 CFR 50.54 "Conditions of Licenses"

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

10 CFR 50.55 "Conditions Of Construction Permits, Early Site Permits, Combined Licenses, And Manufacturing Licenses"

The QA process set out in the HFC QAPM meets the requirements set forth in section (i). The remaining portions of 10 CFR 50.55 will be evaluated on a plant-specific basis.

10 CFR 50.62 "Requirements For Reduction of Risk From Anticipated Transients Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants"

Compliance with this regulation will be assessed on a plant-specific basis.

10 CFR 52.47 "Contents Of Applications; Technical Information."

All HFC test procedures have explicitly stated acceptance criteria, as required in (b)(1).

Other portions of 10 CFR 52.47 will be evaluated on a plant specific basis.

10 CFR 52.80 "Contents Of Applications; Additional Technical Information."

All HFC test procedures have explicitly stated acceptance criteria, and these acceptance criteria 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. The HFC-6000 system's compliance with Defense-In-Depth requirements is detailed in PP901-000-01, Section 8.6.

6.11 CYBER SECURITY

Cyber security of the HFC-FPGA modules is fundamentally the same as the cybersecurity for the original HFC-6000 platform, as detailed in PP901-000-01 Section 8.7. The HFC-FPGA system uses the F-Link, G-Link and RIF as internal communication links, which have a pre-defined message structure and size, and will log any message in the link that deviates from the required size and structure as errors, just as the HFC-6000 ICL performs. 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.

6.12 ISOLATION AND INDEPENDENCE

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

The complete HFC-FPGA modules have been developed in accordance with HFC quality assurance program which complies with NQA-1 2008/2009. The Verification and Validation program for the hardware and software of the modules is compliant with IEEE 1012-2012. In addition, the base platform is designed to be qualified for the use in nuclear safety applications in accordance with EPRI TR 107330 for environmental stress, seismic stress, and isolation qualification Requirements defined in NRC RG 1.180 are used as the basis for EMI/RFI, ESD, and surge withstand qualification tests. Testing for these modules was performed at three locations: [

]

7.1 SYSTEM QUALIFICATION TESTS

7.1.1 Scope

The technical scope and content of EPRI TR 107330 define the basis for the steps involved in completing a generic qualification program. Accomplishing the qualification requires creation of a Test Specimen Application Program (TSAP). The qualification steps are:

a) In addition to the approved equipment list in NRC SE of HFC-6000 Safety Platform, the set of the HFC-FPGA modules listed in Table 1 are assembled.

b) Sets of hardware test modules based on the list in step a) with supporting software are selected to form the Qualification Test Specimen for this amendment to the HFC-6000 Safety Platform.

c) Test Specimen Application Programs (TSAP) are defined and developed for HFC-FCPU and HFC-FCPUX modules of the Qualification Test Specimen. These TSAPs serve as a synthetic application that is designed to aid in the qualification and operability tests for the test specimen.

d) The FCPUs and FCPUXs with their TSAPs and the HFC-FPGA I/O modules are 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.

e) A set of qualification tests to be performed on the Qualification Test Specimen is created, including a defined set of Operability and Prudency tests to be conducted at suitable times in the qualification process. These tests are outlined in VV901-300-09. A top-level description of these tests is shown in Figure 6.

[

]

Figure** 6. **Overall Test Arrangement and Sequence

f) The qualification tests are performed and the results documented. Documentation of results includes definition of the qualification envelope and identification of the specific products that are qualified. A full report of qualification test results is given in TR901-302-01.

This test program intentionally duplicated the detailed 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.

7.1.2 Equipment Tested

A set of the newly developed HFC-FPGA modules as described in Table 1 are assembled into a test specimen. The test specimen is configured to be consistent with the requirements of EPRI TR-107330, Section 4. 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 is developed as new application code using the guidance in BTP-14 and installed in the appropriate modules. Detailed configuration information, a full list

of included hardware, and a detailed description of the TSAP is described in VV901-300-10.

7.1.3 Safety Functions Tested

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

a) The capability of the test specimen to perform defined design functions within specified tolerances under normal environmental and operating conditions.

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, and
- Demonstrate specified levels of Class 1E isolation and continue functioning after application of the test voltage levels.

7.1.4 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 6. 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 are repeated at various points before, during, and after the qualification test to demonstrate that the system performance remained within acceptable limits.

The qualification tests exposed the test specimen to a specifically defined set of abnormal conditions as defined in EPRI TR-107330. The purpose of these tests 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.

7.1.4.1 Test Procedures

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

- TP901-200-01 EPRI TR 107330 Burn-in Test Procedures
- TP901-115-05 VV0115 Integration Test Plan
- 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 Environmental Stress Test Procedure
- TP901-302-03 VV0115 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 Seismic Test Procedure

A master test plan was generated to provide a link between the guidance of the EPRI TR-107330 standard and the procedures that are 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.

7.1.4.2 Test Personnel

All prequalification test activities are conducted by one or more qualified HFC test engineers and test technicians. Qualification tests that require specialized test equipment (e.g., environmental, seismic, and EMI/RFI/ESD/EFT testing) are conducted for HFC by personnel at qualified test facilities. HFC test personnel are present and conduct specified portions of the Operability and Prudency tests during these qualification tests.

7.1.4.3 System Operational Stress Conditions

EPRI TR-107330, Paragraph 6.3.1 identifies the major aging factors associated with a computer-based control system. The following sequence of tests 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 applies 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.
- Isolation test. This test is designed to establish the level of electrical and functional isolation between modules and individual channels inherent in the system design.

Each test exposes the test specimen to abnormal stress conditions while it is powered up and running the TSAP. The EPRI specification and Regulatory Guides provides detailed requirements for test parameters and the order in which particular tests are to be conducted. These requirements are incorporated into the individual test plans and illustrated in the test sequence diagram as shown in in Figure 6.

7.1.4.3.1 Radiation Immunity

The HFC-6000 system and FPGA modules are designed for use in the control room setting per 10 CFR 50 Criterion 19. Due to the low exposure levels required by this environment, no radiation resistance analysis has been performed on the modules in this amendment.

7.1.4.3.2 Seismic Withstand Qualification

Seismic withstand qualification test is generated in accordance with 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 is 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.

7.2 SYSTEM QUALIFICATION TEST RESULTS

7.2.1 Prequalification Tests

The Prequalification Tests consist of the Application Objects test, Burn-In Test, System Setup and Checkout Test, TSAP Validation Test, Operability Tests, and Prudency Tests as shown in Figure 6. Test results are detailed in TR901-302-01 Section 4.6. These tests are required by EPRI TR-107330 Section 5.2.

7.2.2 Operability Tests

The following set of Operability tests is 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 is then used as the basis for evaluating system performance during and/or following each of the qualification tests required by the EPRI standard.

- **Accuracy Test** - This test develops a baseline to compare against the accuracy and linearity of the analog I/O modules observed during the qualification tests.
- **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.
- **Discrete Input Operability Test** - This test verifies the capability of discrete input channels to detect a transition in the input signal being monitored.
- **Discrete Output Operability Test** - This test verifies the capability of discrete output channels to operate reliably within their specified loading conditions.
- **Communication Operability Test** – This test verifies reliable data transfer over the F-Link, RIF, and G-Link.
- **Timer Test** – This test develops the baseline for the timer function accessible to the TSAP.
- **Failure to Complete Scan Test** – This test demonstrates that the system will detect an incomplete scan within one controller operation cycle.
- **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.
- **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 being conducted are detailed in TR901-302-01.

7.2.3 Prudency Tests

The initial execution of the Prudency Tests is performed during the same time period as that of the Operability tests. These tests, as defined by the EPRI standard, do not address any specific requirement but exercise the test specimen in various ways to simulate controller loading. All Prudency tests are executed during the prequalification phase of testing to establish a performance baseline for the test specimen. The following specific tests are defined:

- **Burst of Events Test** - This test is configured to impose a large number of operations on the HFC-FPGA test specimen simultaneously in accordance with EPRI TR-107330, paragraph 5.4.A. This test is automated and is typically run as a continuous background operation for selected qualification tests.
- **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 white noise 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.

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 being conducted are detailed in TR901-302-01.

7.2.4 Qualification Tests

The Qualification Tests consist of the following tests: Environmental, Seismic, EMI/RFI, ESD, and Surge Withstand/EFT/Burst Immunity tests as shown in Figure 6. Portions of the Operability Tests and Prudency Tests are repeated several times throughout these test sequences, as indicated in the detailed test procedure covering each test and as specified in EPRI TR 107330.

7.2.4.1 Environmental Stress Qualification Tests

EPRI TR-107330 requires that the environmental stress test be the first of the qualification tests to be conducted. This test exposes a specially configured HFC-FPGA Test Specimen to extremes of temperature and humidity in order to induce accelerated aging of functional components. It is accomplished by enclosing the Test Specimen in an environmental test chamber. The Test Specimen is running the TSAP throughout the test period, and its operation is monitored by SOE and HAS data loggers located outside the test chamber. In addition, comprehensive functional tests are conducted before, after, and at specified points during the stress testing. The results of these tests are used to identify any deterioration in functional performance of the Test Specimen due to adverse environmental conditions.

The environmental stress test consists of three major phases (Figure 7):

- A minimum 48-hour period with the ambient temperature at 145° F at 95% RH and a transition period of 4 hours during which the ambient temperature is reduced to 35° F at 0% RH (non-condensing).
- A minimum 8-hour period with the ambient temperature at 35° F with 0% (non-condensing).
- A transition period of 4 hours during which the test chamber is brought back to ambient room temperature and humidity.

In addition to the functional modules that make up the Test Specimen, hot spares are placed inside the test chamber, and they remained powered up throughout the entire test. In accordance with EPRI TR 107330, failing modules could be replaced by these hot spares during the stress periods before operability tests checkpoints. 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 periods mandated are depicted in Figure 7.

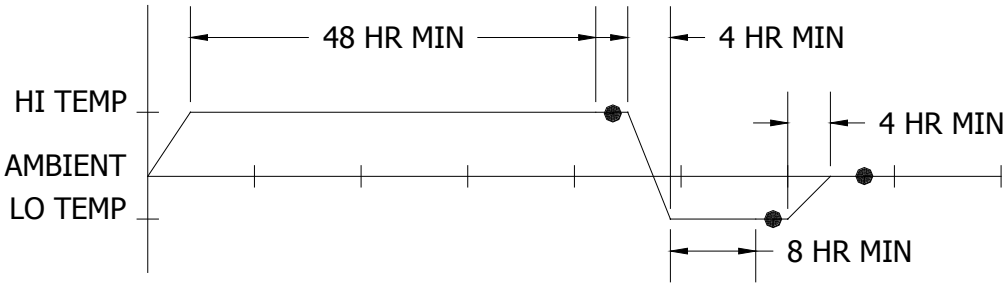

Figure** 7. **Environmental Stress Test Profile

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 are maintained. Details of the results of this test are discussed in TR901-302-01 Section 5.

7.2.4.2 EMI/RFI Qualification Tests

The HFC-FPGA VV0115 Test Specimen is designed to operate in a wide variety of industrial applications. Both the HFC system hardware and the field equipment generate electromagnetic radiation (noise). The operation of the HFC system is 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. Details of this testing are discussed in TR901-302-01 Section 8.

7.2.4.3 ESD Test

Components of an HFC-FPGA control system may be installed in an electrical equipment room as well as at various locations near the field equipment under control. In either case, the potential exists for exposure of sensitive electronic components to high voltage electrostatic discharges (ESD). This test subjects each component of the HFC-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 are defined by IEC 64000-4-2. Overall acceptance criteria specified by the EPRI specification are as follows:

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

Details of the test results are discussed in TR901-302-01 Section 9.

7.2.4.4 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 is to demonstrate that Test Specimen performance characteristics remain within acceptable limits during and after exposure to such discharges. The Test Specimen is powered on and running the TSAP when the test pulses are being applied to specific circuits in accordance with EPRI TR-107330. Three tests were conducted: EFT, Combination Wave, and Ring Wave. Details of the test results are discussed in TR901-302-01 Section 9.3.

7.2.4.5 Seismic Stress Test

Seismic testing exposes the Test Specimen to a set of dynamic spectra designed to simulate an Operating Basis Earthquake (OBE) and a Safety Shutdown Earthquake (SSE). This test spectrum defined by EPRI TR-107330 is shown in Figure 8. The dynamic spectra consists 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 overall scope of testing consists 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 are run throughout the test sequence.

Performance during these tests is monitored by a combination of:

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

A preliminary resonance test is conducted to determine if the Test Specimen components has any resonant frequencies within the RRS. The test is conducted by imposing a low level sinusoidal sweep. If one or more resonant frequencies are detected, the Test Response Spectrum (TRS) is to be centered on the resonant frequency that produced the maximum response in the Test Specimen. Overall requirements for the resonance search are governed by IEEE Std 344.

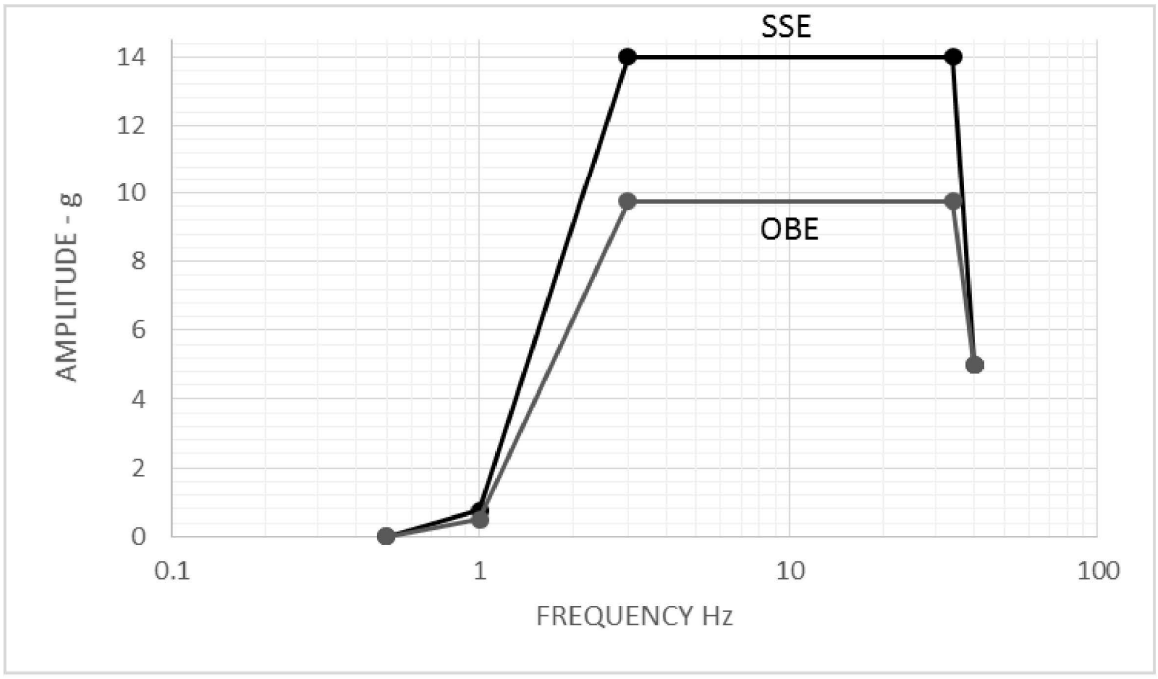

Figure 8. Seismic Test Spectrum

All dynamic seismic tests are conducted using the TRS established as the result of the resonance sweep test. 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 any particular dynamic test is in progress, an HFC test engineer runs the specified combination of automated tests to verify overall system performance. Following each dynamic test, the entire Test Specimen is examined for mechanical damage. Any mechanical damage sustained during testing was recorded and subsequently reported in detail in the seismic test report. Detailed results of this testing are discussed in TR901-302-01 Section 10.

7.2.5 Post Qualification Tests

The Post Qualification Tests consisted of re-running complete Operability and Prudency tests at the HFC Facility after completion of all qualification testing. The purpose of the

Post Qualification Tests are 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 are 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 test results are detailed in TR901-302-01, Section 11.

7.2.6 Test Results

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 when applicable. A final summary of test results is detailed in TR901-302-01, Section 12. The Test Specimen was found to have operated normally during and following all qualification testing.

8.0 CONCLUSION

The HFC-FPGA system platform implements the functional characteristics of the HFC-6000 system platform using FPGA architecture. The design and implementation of the HFC-FPGA system platform has followed discipline specifications and development lifecycle process that meet the requirements of the 10 CFR 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 systems are functionally the same as the PLCs.

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