DOOSAN

HF Controls

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

RR901-107-10 Rev B

Effective Date: 6 / 3 / 2016

Prepared By: Eugene O'Donnell

Reviewed By: Gordon Ngo

Approved By: Steve Yang

[redacted]

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

Table of Contents

List of Figures

Number **Title** **Page**

List of Tables

Number **Title** **Page**

1.0 PURPOSE AND SCOPE

The HFC-6000 FPU System 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 Control System 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-FPU 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-FPU I/O modules (TMR configuration).

The present amendment to the HFC-6000 Safety platform covers only the central controller architecture. The resulting HFC-FPU 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.

2.0 HFC-FPGA CONTROL SYSTEM OVERVIEW

The HFC-6000 FPU System consists of a set of PCBs using the HFC-6000 form factor and the I/O connector arrangement so that any HFC-FPU module can be inserted into any I/O slot of an HFC-6000 expansion rack. The complete set of HFC-FPU modules includes controllers, I/O modules, and the HSIM F-Link High Speed Interface 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. (The FPC08 Gateway Controller modules were previously qualified and are not included in the present amendment to the Topical Report.)

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-FPU 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. 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. To ensure the HFC-FPU 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.

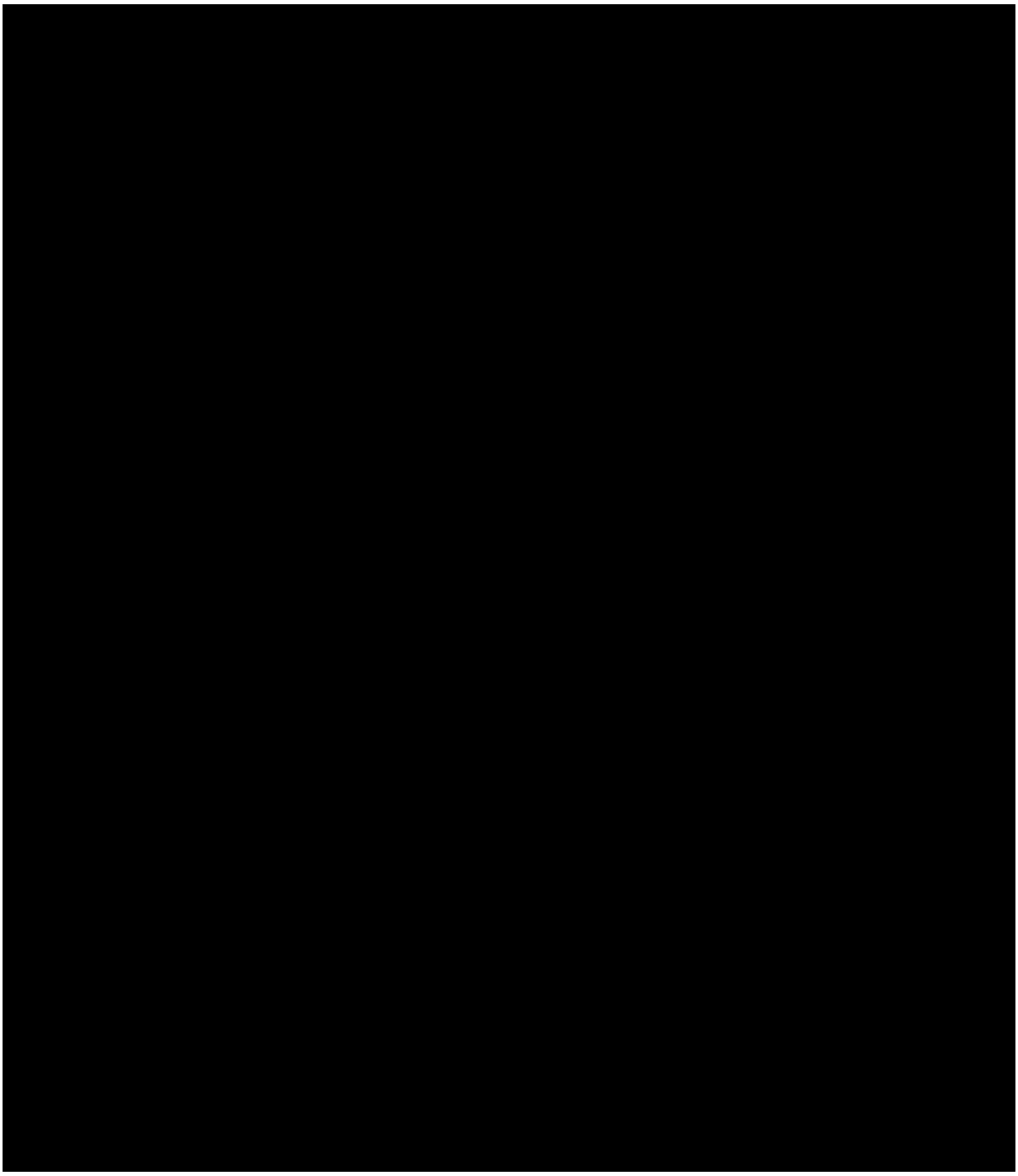


Figure** 1. **Test Specimen Equipment Block Diagrams

Table 1. Qualification Modules

Part Number	Module Name	Description
40117481	HFC-FPUD01	FPU I/O Module for 16 DI Channels and 16 DO Channels
40117482	HFC-FPUD02	FPU I/O Module for 32 DI Channels
40124281	HFC-FPUA01	FPU I/O Module for 16 4- to 20-mA AI Channels
40129481	HFC-FPUAO	FPU I/O Module for 8 4- to 20-mA AO Channels
40127081	HFC-FPUL	FPU I/O Module for 8 AI Channels for Type E Thermocouples
40127481	HFC-FPUM	FPU I/O Module for 8 AI Channels for 100-Ohm Platinum RTDs
40145781	HFC-FPUM2	FPU I/O Module for 8 AI Channels for 100-Ohm Platinum RTDs
40132281	HFC-FCPU	CPU for the FPU Controller product line
40145281	HFC-FCPUX	CPU for the FPU Controller product line
40108689	HFC-HSIM	F-Link High Speed Interface Module

2.1 SYSTEM COMPONENTS

As indicated in Table 1, there are ten different modules covered by the present amendment, and 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. The FPUM and FPUM2 modules are comprised of different hardware but are directly interchangeable in pinout, function, and operation. All of the FPU module designs are based on two FPGA modules – a Process FPGA and a Diagnostic FPGA. The Process 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 Process 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 Process FPGA and the correct monitored signals from the Diagnostic FPGA for the process to proceed. Both the Process 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.

- Process 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 CPU 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-FPU 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 CPU modules control status transfer to the Gateway.

2.2 VERFICATIONS AND VALIDATIONS

All HFC product development lifecycles are conducted in accordance with HFC quality process procedures which are NQA-1 1994 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 fully compliance with the IEEE 1012-2004 revision.

2.3 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
h. Test Specimen Post Test

Test results demonstrate overall functional capabilities of each module included in the test program. Refer to Section 6 for detailed coverage of the test program and test results for each module.

3.0 REFERENCES

3.1 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.

FPU Module. An HFC-6000 PCB as listed in Table 1 and containing two subcategories: FPU controller module and FPU I/O module.

Life-Cycle 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 are verified fully.

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

3.2 SPECIAL TERMS AND ABBREVIATIONS

A	Ampere
AC	Alternating Current
ACE	Abnormal Conditions and Effects
ADC	Analog/Digital Converter
AI	Analog Input
AO	Analog Output
AUX	Auxiliary
BOE	Burst of Events
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
EFT	Electric Fast Transient
EMI	Electro-Magnetic Interference
EPRI	Electric Power Research Institute
ESD	Electrostatic Discharge
EWS	Engineering Workstation
F	Fahrenheit
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 and the Communication Gateway
HAS	Historical Archiving System
HFC	HF Controls
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
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
NC	Normally Closed
NO	Normally Open
NRC	Nuclear Regulatory Commission
OBE	Operating Basis Event
PCB	Printed Circuit Board
QA	Quality Assurance
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
SE	Safety Evaluation
SPM	Software Program Manual
SOE	Sequence of Events
SSE	Safety Shutdown Event
Std	Standard
TC	Thermocouple
TPM	Tri-Ported Memory
TR	Topical Report
TRS	Test Response Spectrum
TSAP	Test Specimen Application Program
v/V	Volts
w	Watt

4.0 CODES, STANDARDS, REGULATIONS, GUIDANCE AND REFERENCES

4.1 CODES, STANDARDS, REGULATIONS AND GUIDANCE

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.

4.1.1 Industry Standards

ASME NQA-1/NQA-2	"QA of Design Software", 1994/1995
EPRI TR-102323	Guidelines for Electromagnetic Interference Testing of Power Plant Equipment, Rev.2
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 323	"IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations", 2003
IEEE Std 344	"IEEE Standard for Seismic Qualification of Class I 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 Class 1E Systems", 2000
IEEE Std 472	"Guide for Surge Withstand Capability Tests", 1974
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	"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", 1983
IEEE Std 830	"IEEE Standard Guide for Software Requirements Spec.", 1984
IEEE Std 1008	"IEEE Standard for Software Unit Testing", 1987
IEEE Std 1012	"IEEE Standard for Software Verification and Validation Plans", 2004
IEEE Std 1016	"Recommended Practice for Software Design Description", 1987
IEEE Std 1028	"Standard for Software Reviews and Audits", 1998
IEEE Std 1042	"IEEE Guide to Software Configuration Management", 1987
IEEE Std 1074	"IEEE Standard for Developing Software Life Cycle Processes", 1995
IEEE Std 1228	"IEEE Standard for Software Safety Plans", 1994
MIL-STD-461E	"Measurement of Electromagnetic Interference Characteristics"

4.1.2 NRC Regulations and Guidance

10 CFR Part 21	"Reporting of Defects and Noncompliance"
10 CFR Part 50, App B	"Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants"
10 CFR Part 50.36	"Technical Specifications"
10 CFR Part 50.49	"Environmental qualification of electric equipment important to safety for nuclear power plants"
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

BTP 7-11	"Guidance for Application and Qualification of Isolation Devices", Rev. 5, 2007
BTP 7-14	"Branch Technical Position: Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems", Rev. 5, 2007
BTP 7-17	"Guidance on Self-Test and Surveillance Test Provisions", Rev.5, 2007
BTP 7-19	"Guidance for Evaluation of Defense-in-Depth and Diversity in Digital-Based I&C Systems", Rev. 5, 2007
BTP 7-21	"Guidance on Digital Computer Real-Time Performance", Rev.5, 2007

Regulatory Guide

RG 1.22	"Periodic Testing System Actuation Functions", 1972

RG 1.29	"Seismic Design Classification", 2007
RG 1.47	"Bypassed and Inoperable Status Indications for Nuclear Power Plant Systems", 1973
RG 1.53	"Application of the Single Failure Criterion to Nuclear Power Plant Systems", 2003
RG 1.62	"Manual Initiation of Protective Actions", 1973
RG 1.75	"Physical Independence of Electrical Systems", 2005
RG 1.89	"Qualification for Class 1E Equipment 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 1.118	"Periodic Testing of Electric Power and Protection Systems", 1995
RG 1.152	"Criteria for Use of Computers in Safety Systems of Nuclear Power Plants", 2006
RG 1.153	"Criteria for Safety Systems", 1996
RG 1.204	"Lightning Protection", 2005
RG 1.209	"Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants", 2007
RG 1.168	"Verification, Validation, Reviews, and Audits for Digital Computer Software Used In Safety Systems of Nuclear Power Plants", 2004
RG 1.169	"Configuration Management Plans for Digital Computer Software Used In Safety Systems of Nuclear Power Plants", 1997
RG 1.170	"Software Test Documentation for Digital Computer Software Used In Safety Systems of Nuclear Power Plants", 1997
RG 1.171	"Software Unit Testing for Digital Computer Software Used In Safety Systems of Nuclear Power Plants", 1997
RG 1.172	"Software Requirements Specifications for Digital Computer Software Used In Safety Systems of Nuclear Power Plants", 1997
RG 1.173	"Development Software Life Cycle Processes for Digital Computer Software Used In Safety Systems of Nuclear Power Plants", 1997
RG 1.180	"Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems", 2003
RG 5.71	"Cyber Security Programs for Nuclear Facilities", January 2010

4.1.3 HFC Technical Documents

DS001-007-01	HFC-FPGA Controller System Component Design Description, Rev A
DS001-007-02	FPGA F-Link Communication Component Design Description, Rev A
DS001-007-03	FPGA Controller Logic Library Component Design Description, Rev A
DS901-001-74	HFC-FCPU Hardware Design Specification, Rev A
DS901-007-04	HFC-FCPU Software Design Specification, Rev A
DS002-000-01	C-Link Design Specification, Rev. D
DS901-001-54	HFC-FPUD Hardware Design Specification, Rev B
DS901-001-70	HFC-FPUA Hardware Design Specification, Rev B
DS901-001-71	HFC-FPUL Hardware Design Specification, Rev A
DS901-001-72	HFC-FPUAO Hardware Design Specification, Rev B
DS901-001-73	HFC-FPUM Hardware Design Specification, Rev A
DS901-002-19	HFC-FPUM2 Design Specification, Rev A
DS901-002-18	HFC-FCPUX Hardware Design Specification, Rev A
DS901-003-01	HFC-FPUD Software Design Specification, Rev A
DS901-003-02	HFC-FPUA Software Design Specification, Rev A
DS901-003-03	HFC-FPUL Software Design Specification, Rev A
DS901-003-04	HFC-FPUAO Software Design Specification, Rev A
DS901-003-05	HFC-FPUM Software Design Specification, Rev A
MS901-000-08	HFC-FPGA System Design Specification, Rev A
TR901-302-01	VV0115 Pre-Qualification Test Report, Rev A
TR901-302-02	VV0115 Environmental Stress Test Report, Rev A
TR901-302-03	VV0115 EMI RFI Test Report, Rev A
TR901-302-04	VV0115 Surge Withstand Test Report, Rev A
TR901-302-05	VV0115 Electrostatic Discharge Withstand Test Report, Rev A
TR901-302-06	VV0115 Seismic Test Report, Rev A
TR901-302-07	VV0115 Isolation Test Report, Rev A
TR901-302-08	VV0115 Post-Qualification Test Report, Rev A

4.1.4 HFC-6000 NRC Reviewed Documents

ML080780170	HFC-6000 Safety System Topical Report, Rev. C
ML100820253	HFC-6000 Radiation Exposure Evaluation, Rev. A

ML110831014 NRC Safety Evaluation Report of HFC-6000 Safety Platform

ML111990323 ERD111 Qualification Retest Summary Report, Rev. A

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

4.1.5 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

5.0 HFC-FPGA CONTROL SYSTEM HARDWARE/SOFTWARE

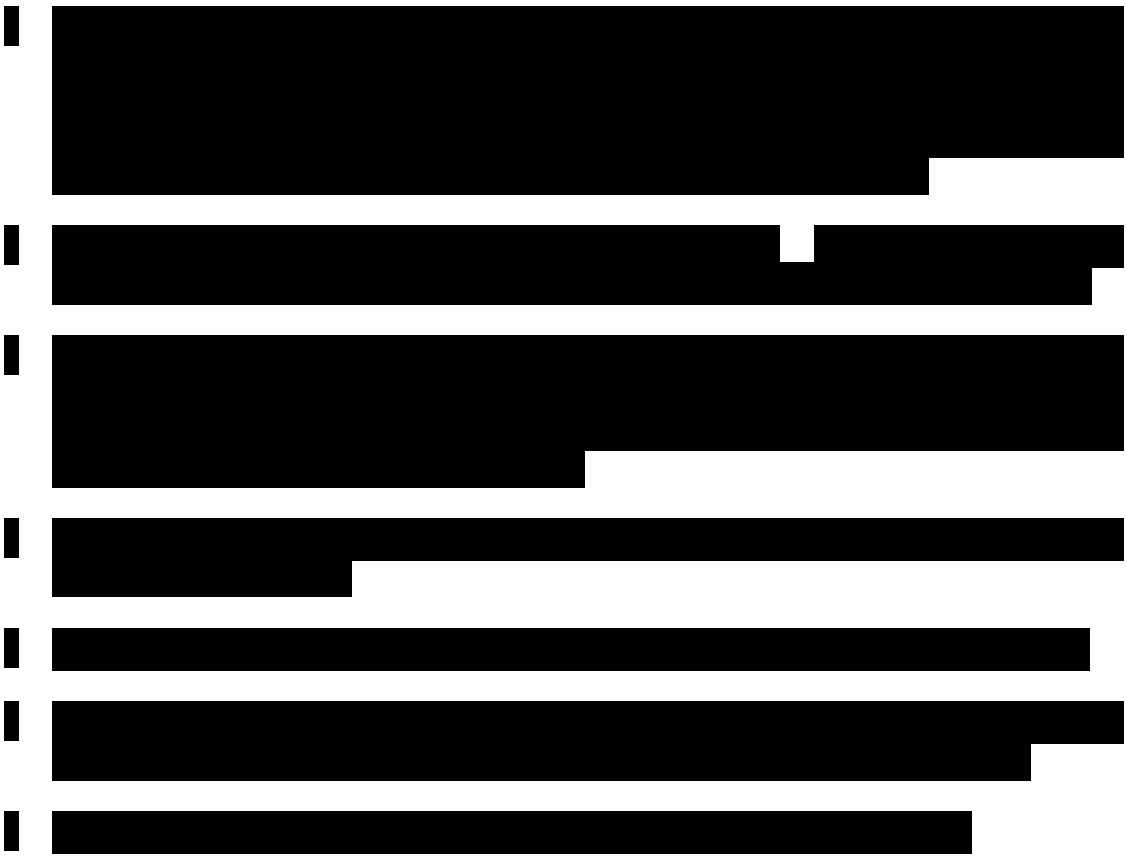
All of the FPU modules covered by this amendment share the same hardware and software architecture. The major differences from one module to the next consist of the following:

- Hardware interface for a particular type of signals from field equipment
- 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-FPU I/O modules 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.

5.1 HARDWARE ARCHITECTURE

5.1.1 Common Kernel

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



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.

5.1.3 Power Distribution

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.

All power lines configured for a particular rack land at a common power disconnect,

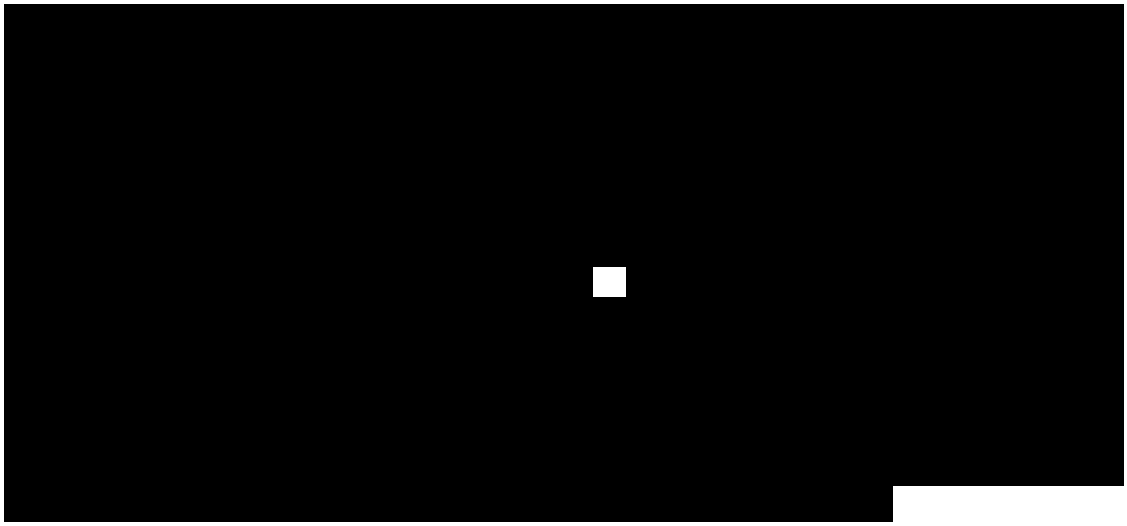
and they are routed from that point to each backplane connector. Every I/O connector in the rack receives the same combination of redundant power rails, and onboard hardware performs diode auctioneering and voltage regulation. In contrast, analog or digital channels requiring external excitation power receive Aux power from the I/O interface, and these power traces are isolated from everything else on the assembly.

5.1.4 Communication Links

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

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 FPU 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-FPU Control System includes multiple racks, connection between the racks 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 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.

5.2 APPLICATION CONTROL

In previous implementations of the HFC-6000 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 CPU modules have the capability of executing application code. All control functions will reside in the CPU, 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 accumulated status to the CPU via the F-Link during their mastership period. The primary CPU executes the application code and distributes the updated status images to output modules and the secondary CPU. The output modules receive updates of processed data, execute their function, and transfer those data to the output points under their control. The redundant CPU controls regular transfer of status to the Gateway module via the G-Link, and the Communication Gateway broadcasts the accumulated status to the C-Link during its mastership.

5.3 SOFTWARE ARCHITECTURE

Every HFC-FPU module PCB includes two FPGAs that operate in lock-step with one another. Figure 3 illustrates the general arrangement of both an FPU I/O module and an FPU controller module. The Process FPGA contains the code that executes all control functions; the Diagnostic FPGA executes diagnostics during execution of those control functions. Since the two FPGA modules are designed to operate in lock-step, they must remain synchronized with one another in order for any process to be completed without failure. Detection of processing failures are logged and generate error status messages that are included with the data broadcasts to the F-Link. Loss of synchronization between the Process and Diagnostic FPGAs is fatal and will force a watchdog timeout.

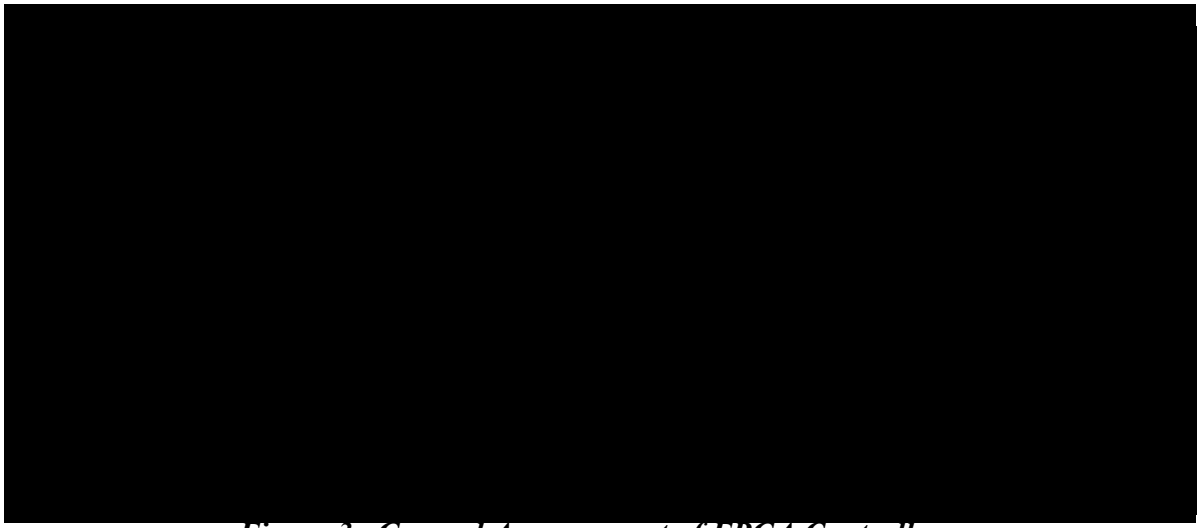


Figure 3. General Arrangement of FPGA Controllers

5.3.1 Process FPGA Software for HFC-FPU Controllers

The software for the Process 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 FPU module. For detailed information about the common library modules, refer to DS001-007-001.

F-Link Control Modules. The F-Link control modules create the token-passing protocol for the HFC-FPU 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 DS001-007-002.

I/O Interface Control Modules. Because each of the HFC-FPU 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 FPU 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 CPU assemblies. Refer to DS901-007-04 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 DS901-007-04 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 a combinatorial logic module. The binary file and combinatorial logic utility files are generated by an HFC software tool called One-Step during development of a specific application. Processing functions available include Boolean logic, analog algorithms, and arithmetic operations. The application processing FSM performs the block operations identified in the flash binary file and combinatorial logic module during normal operation of the control system. Refer to DS001-007-003 for the library of application-related modules supported by the present implementation of the HFC-6000 FPGA system.

5.3.2 Diagnostic FPGA Software

The Diagnostic FPGA software controls diagnostic functions for each process controlled by the Process FPGA. The Process and Diagnostic FPGAs are connected to one another by the HPI. Each time the Process FPGA initiates an operation, it informs the Diagnostic FPGA via the HPI. When the Process FPGA produces discrete control signals, both the hardware on the board and the Diagnostic FPGA receive the same signals. The Diagnostic FPGA then inverts the control signals and both the signals from the Process FPGA and the inverted control signals from the Diagnostic FPGA are required for the process to execute. Finally, when an HFC-FPU receives data, both the Process and the Diagnostic FPGAs receive the same data via different hardware paths. The two FPGAs then exchange their data images to verify that both received the same data. If there is any discrepancy between the two, then the data is rejected as invalid. Refer to the software design specification for individual HFC-FPU modules for more detailed information about specific software modules and functions performed by the Diagnostic FPGA Software.

6.0 EQUIPMENT QUALITIFCATION

The complete HFC-6000 FPGA controllers have been developed in accordance with HFC quality assurance program which complies with NQA-1 1994/1995. The Verification and Validation program for the hardware and software of the controllers 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.

6.1 SYSTEM QUALIFICATION TESTS

6.1.1 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-FPU 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 FPU 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.

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.

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.

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 hardware design will meet or exceed the capabilities of that platform.

6.1.2 Equipment Tested

A set of the newly developed HFC-FPU modules *(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. Qualification Test Reports document the tests results and related analyses. 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 requirements for the individual modules in the test specimen and the TSAP are described in a TSAP Requirements Specification. Detailed configuration information, such as module serial numbers and software versions, are recorded in a Master Configuration List (MCL).

6.1.3 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:

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

2. The capability of the test specimen to perform design functions within specified tolerances under the stressed conditions defined in EPRI TR-107330, Sections 5 and 6. Specific stress conditions demonstrated the capability of the test specimen to:

   - Function during and after exposure to abnormal temperature and humidity
   - Function during and after 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
- Function under varying conditions of source power quality
- Demonstrate specified levels of Class 1E isolation and continue functioning after application of the test voltage levels.

6.1.4 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 4. 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.

6.1.4.1 Test Procedures

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

- Burn-in Test
- System Setup and Checkout Test
- TSAP Validation Test
- Operability Test
- Prudency Test
- Environmental Stress Test
- Seismic Stress Test
- EMI/RFI Test
- ESD Test
- EFT/Burst Immunity Test
- Surge Withstand Test
- Isolation Test

Figure 4. Overall Test Sequence

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, and it includes a separate test plan for each qualification test to be performed. The test procedure for each test identifies requirements, testing criteria, acceptance criteria, and documentation for a particular test. The test procedures provide step-by-step instructions for conducting the tests and recording the results. These instructions include setup of equipment, test equipment requirements, environmental requirements, and procedural steps for conducting the tests, acceptance criteria, and tolerances. 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
- 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.

6.1.5 Test Sequence

As illustrated in Figure 4, the test program consists of separate prequalification, qualification, and post qualification test phases. The requirements, design, manufacture, and assembly phases of the life cycle are completed prior to the start of the qualification testing in accordance with HFC procedures. Actual testing of the test specimen commences with system integration. The prequalification phase is conducted by HFC test personnel at the HFC facility in Texas. The qualification tests may be conducted at several different test facilities, as detailed in the test reports. The overall sequence of the test program is as follows:

1. Configure test specimen components in accordance with applicable engineering drawings and HFC procedures at the HFC facility.
2. Conduct the Application Object Tests, Burn-in Test, TSAP Verification, and Integration (Setup and Checkout) Procedure to prepare and validate the test specimen and Test System.
3. Run the Operability and Prudency prequalification tests at HFC facility.
4. Disassemble test specimen and ship it to a certified test facility for qualification testing.
5. Reassemble test specimen at the test facility and verify its functional operation. The test procedure for each of the qualification tests defines required functional verification of the test specimen before the start of the actual qualification test.
6. Perform designated stress tests in accordance with separate test procedures. The Test specimen is disassembled and shipped back to the HFC facility after qualification testing is complete.
7. Reassemble the test specimen at HFC facility and verify correct assembly and interconnection of all components.
8. Conduct Operability and Prudency tests after completion of all qualification tests.

Detailed instructions for conducting the specific tests are contained in separate test procedures. Test results and the associated analyses are refined in individual test reports.

6.1.5.1 Test Arrangement and Methodology

The test arrangement consists of the test specimen connected to the HPAT controller and a PC workstation that are separate from the test specimen. The HPAT tester consists of a separate HFC controller equipped with a test application program and a set of I/O modules configured to provide simulated inputs for the test specimen. The PC workstation is equipped with a standard set of HFC interactive graphics and data logging

software tools that are linked to both the HPAT and to the test specimen. This arrangement permits the test engineer to start/stop selected test routines and to record test results in the HAS and SOE data loggers. During the prequalification testing phase, the test specimen is configured and subjected to a series of hardware, software, and functional tests. The same TSAP is installed in both test specimen CPUs, and its functional operation is verified. The total TSAP includes a set of simulated applications for safety system functions as well as algorithms specifically developed to support Operability and Prudency testing. The purposes for this phase of testing are as follows:

- Establish functionality of the software objects available to the TSAP.
- Verify functional operation of the TSAP.
- Validate operation of the automated test sequences.
- Establish an operational baseline for the test specimen.
- Document calibration and linearity of AI and AO modules included in the test specimen.

During the qualification tests, the test specimen is subjected to stress conditions to simulate various aging factors. While each test is in progress, the TSAP is processing test signal waveforms supplied by the HPAT. Responses of the test specimen during each qualification test are logged for comparison with the performance baseline established during prequalification testing to detect any degradation in performance. After all of the qualification stress tests are completed, Operability and Prudency tests are repeated, and all responses are recorded for subsequent evaluation. In each case, the logged responses of the test specimen provide the objective basis for evaluating the performance of the generic modular control system design.

6.1.5.2 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.

6.1.5.3 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:
    1. It measures the amplitude of electromagnetic energy radiated by the system over specified frequency ranges; and

2. 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.

6.1.5.3.1 Radiation Immunity

The HFC-6000 system is 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.

6.1.5.3.2 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.

6.2 SYSTEM QUALIFICATION TEST RESULTS

6.2.1 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 4.

6.2.1.1 Application Object Test

According to EPRI TR-107330, Paragraph 5.2.A, the term *Application Objects* refers to individual program algorithms in a common library that can be assembled to create an application program. For the HFC-6000 product line, these items correspond to the program algorithms for CQ4 blocks, timers, etc. At the present time a subset of the total HFC-6000 library modules have been re-coded in Verilog to run on the FPU controllers. (Refer to DS001-007-03 FPGA Controller Logic Library Component Design Description, Rev A.) The Application Object tests for these algorithms are covered by the detailed V&V review and testing program.

6.2.1.2 Burn-in Test

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

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

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

6.2.1.3 System Setup and Checkout

The System Setup and Checkout Tests are performed to verify that the project-specified hardware, wiring, and communication cabling were installed correctly, that all power sources are operational, and that C-Link, F-Link, RIF, and G-Link communication has been established before executing the TSAP Validation Test. Included in the scope of this testing are the following activities/results:

- Verifies that all specified components of the test specimen were received, correctly installed, and functionally tested in accordance with project documentation requirements.
- Verifies that the correct software has been installed in test specimen, HPAT, and HPAT computer. This is done as part of the TSAP Validation Test Procedure.
- Performs Continuity Testing to confirm that all interconnection wiring is correctly installed.
- Verifies that data transmission has been established.
- Verifies that communication has been established over the F-Link, RIF, and G-Link within the test specimen and the C-Link connected to the HPAT.
- Verifies that all HFC-FPU PCBs are functional and communicating with one another.

6.3.1.4 TSAP Validation Test Procedure

Both primary and secondary HFC-FCPU and HFC-FCPUX controllers had a TSAP installed that included sample control logic for power plant processes as well as logic to

support automated qualification testing. The TSAP Validation Test Procedure validated the following activities:

- **Source Code Verification** – The source code file generated by the HFC One-Step utility is examined line by line and compared with the graphic representation of the associated logic diagrams.
- **Loop Logic Test** – This test verifies the functional operation of the logic for each sample control loop based on the algorithm in the TSAP logic diagrams.
- **Operability Test Support** - This test verifies the functional operation of the TSAP code designed to support Operability testing and verifies that the test approach would produce the expected data. The automated Operability tests are controlled by application code installed in the HPAT. Validation of the automated logging of test results is accomplished during the first execution of the Operability tests.
- **Prudency Test Support** - This test verifies functional operation of the TSAP code designed to support the automated Prudency tests. The automated Prudency tests are controlled by application code installed in the HPAT. Execution of this test excludes automated logging of test results, which is accomplished during the first execution of the Prudency tests.

Functional testing of the TSAP code is conducted after completion of the test specimen Integration (Setup and Checkout) Procedure in accordance with EPRI TR-107330, Paragraph 5.2.C.

6.2.2 Operability Tests

The following set of Operability tests is performed following completion of the TSAP tests described above. 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.

All tests are performed in accordance with their respective operability test procedures for each test specimen.

6.2.3 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-FPU 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.

6.2.4 Qualification Tests

The Qualification Tests consist of the following tests: Environmental, Seismic, EMI/RFI, ESD, Surge Withstand/EFT/Burst Immunity, and Isolation tests as shown in Figure 4. 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.

6.2.4.1 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-FPU 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 5):

- 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 5.

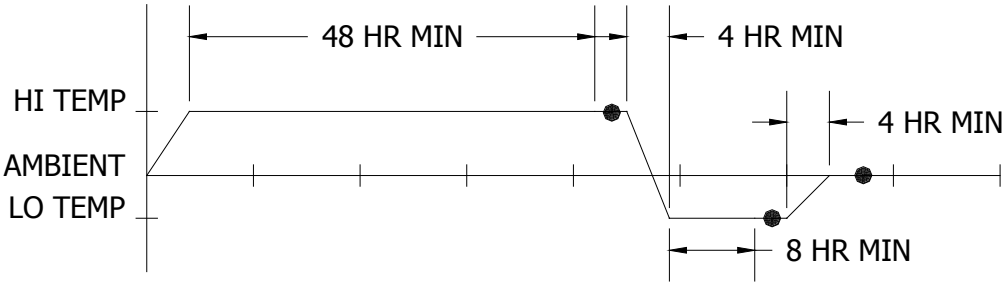


Figure 5. Environmental Stress Test Profile

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. In the rest of this report, the humidity conditions are implied by the temperature and will not be mentioned again. These validation tests are grouped into Operability and Prudency tests in accordance with EPRI TR 107330. Refer to the standard for the details of these test descriptions.

6.2.4.1.1 Test Points/Required Validation Tests

In accordance with EPRI TR 107330, Operability and Prudency tests are executed at defined points as specified. Table 2 below is an excerpt from Table 5-1 of the EPRI TR 107330 specification and indicates the specific combination of tests required.

***Table** 2. Required Operability and Prudency Tests during Environmental Test*

Environmental Test Points	Operability Tests	Prudency Tests
1. End of High Temp/High RH 2. End of Low Temp/Low RH 3. Back to ambient condition	At all test points	At the end of high temp/high RH only

6.2.4.1.2 Operability Tests

The following are the operability tests which are executed at each of the environment stress test point:

1. Accuracy
2. Response Time
3. Discrete Input Operability
4. Discrete Output Operability
5. Communication Operability
6. Timer
7. Failure to Complete Scan Detection
8. Failover Operability
9. Loss of Power
10. Power Interruption/Power Quality

6.2.4.1.3 Prudency Tests

The burst of event (BOE) tests are executed at the end of low temperature/low relative humidity.

6.2.4.2 EMI/RFI Qualification Tests

The HFC-FPU 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. The test sequence covered a series of four separate tests. During the first two tests, the Test Specimen is exposed to an external source of EMI/RFI, and the functional operation of the equipment is examined for signs of degraded operation. During the remaining two tests, the Test Specimen is configured for normal operation, and the magnitude of electromagnetic radiation generated by the equipment is measured.

6.2.4.2.1 Required EMI/RFI Test Sets

In accordance with NRC RG 1.180, the following EMI/RFI tests are required for validating system electromagnetic emission and immunity limits. See Table 3.

Table 3. Required EMI/RFI Tests

Description	Testing Method	Test Signal Range
Low Frequency Conducted Emission	MIL-STD-461E CE101	60 Hz/120Hz to 10 kHz
High Frequency Conducted Emission	MIL-STD-461E CE102	10 kHz to 2 MHz
Low Frequency Radiated Emission	MIL-STD-461E RE101	30 Hz to 100 kHz
High Frequency Radiated Emission	MIL-STD-461E RE102	2 MHz to 10 GHz
Magnetic Field Radiated Susceptibility	ML-STD-416E RS101	30 Hz to 100 kHz
Electric Field Radiated Susceptibility	ML-STD-416E RS103	30 MHz to 10 GHz
Low Frequency Conducted Susceptibility (Power Lines)	MIL-STD-461E CS101	30 Hz to 150 kHz
High Frequency Conducted Susceptibility (Power Lines & Signal Lines)	MIL-STD-461E CS114	10 kHz to 30 MHz
Conducted Susceptibility Bulk Injection (Signal Lines)	MIL-STD-461E CS115	EFT Bulk Injection at 2A
Conducted Susceptibility, Damped Sinusoidal Transient (Signal Lines)	MIL-STD-461E CS116	10 kHz to 100 MHz
Surge Withstand (Power Lines)	IEC 61000-4-4 IEC 61000-4-5 IEC 61000-4-12	Ring Wave, Combination Wave, EFT 2kV and 4kV
Electrostatic Discharge Immunity	IEC 61000-4-2	8kV Contact, 15kV Air

6.2.4.2.2 Required System Validation Tests

Automated Operability and Prudency tests developed for validating the functionality of the test specimen are used. According to EPRI TR 107330 Section 4.3.7 EMI/RFI Withstand Requirements, when the PLC modules are subjected to EMI/RFI disturbances, the PLC modules shall perform as follows:

1. The main and any coprocessors shall continue to function
2. The transfer of I/O data shall not be disrupted.
3. The emissions shall not cause the discrete I/O to change state.
4. Analog I/O level shall not vary more than ±3%.
5. Susceptibility will not be tested at levels below 100% unless a failure occurs at 100% signal strength.

In addition, the system shall continue to provide the following performance:

1. Response Time

   The response time for digital I/O and Analog I/O shall be within the manufacturer's acceptance limits. For the TSAP running on the system, the acceptance limits for analog response time is < 350ms and for digital response time is < 300ms.

   Note: This response limit is not a performance benchmark for nuclear control systems. Particular systems may require a faster response time.

2. Discrete I/O Operability
   All states of the discrete input shall be detected and all changes of the discrete output shall occur.
3. Timer Function
   Accuracy of the timer function shall stay within ±0.1%.
4. Communication Operability
   Communication performance shall meet the manufacturer's acceptance limits. No increase in errors shall be reported for F-Link, RIF, or G-Link communication.
5. Burst of Event (BOE) Operability
   All transitions of the states of all channels driven by the BOE shall be detected. Analog I/O levels shall not have variations greater than ±3%.

6.2.4.3 ESD Test

Components of an HFC-6000 control system may be installed in an electrical equipment room as well as at various locations near the field equipment under control. In either case, the potential exists for exposure of sensitive electronic components to high voltage electrostatic discharges (ESD). This test subjects each component of the HFC-FPU 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.

6.2.4.4 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.

6.2.4.4.1 Surge Withstand Test Sets

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

- Application of surge waveform shall not damage any module, component, or channel other than those specific modules or circuits subjected to the test waveform.

- Channels or modules other than the one under test shall continue to operate within normal accuracy limits for those modules during and after application of the test waveform.
- Failure of a single controller of the redundant pair will not be considered a failure condition if the backup controller assumes normal operation for the test specimen.
- Failure of the particular channel or circuit under test will not be considered a failure of the test specimen if the circuit (e.g., power module) is redundant, if the failure does not disrupt overall operation of the test specimen, or the failure does not propagate to other channels or circuits.

6.2.4.5 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 6. 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
- Post seismic test inspection and operability test.

Various Operability and Prudency tests are run throughout the test sequence. Performance during these tests is monitored by a combination of:

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

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 6. 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. The response spectrum of the Test Specimen is reported for 0.5%, 1.0%, 2.0%, 3.0%, and 5.0% damping factors. 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 is to be recorded and subsequently reported in detail in the seismic test report.

6.2.4.6 Seismic Test Sequence

The overall sequence of the seismic test proceeded as follows:

1. Install the Test Specimen on the seismic actuator table. The HPAT and monitoring equipment are mounted next to the seismic actuator table with the communication and I/O cables secured to support structures.

2. Seismometers are mounted at designated points on the test specimen.

3. Following installation, Operability and Prudency tests are run to verify that the Test Specimen is fully operational.

4. Test facility personnel run the resonance search to establish the overall test spectrum.

5. Five OBE tests are run consecutively. Following each test run, the Test Specimen is inspected for damage, loose cables, or loosened fasteners. Any damage is

documented, and repairs are performed as required prior to the start of the next test run.

6. The SSE Test is run.

7. Following the SSE test the Operability and Prudency tests are run to record the final performance characteristics of the Test Specimen.

6.2.4.7 Isolation Test

IEEE Standard 384-1992 mandates isolation between Class 1E and non-Class 1E electrical components within a safety-critical control system. EPRI TR-107330 paragraph 4.3.2 specifies different levels of group-to-group isolation for each type of I/O circuit addressed by the specification, and EPRI TR-107330 paragraph 4.6.4 specifies the minimum level of isolation required between modules. The purpose for this isolation is twofold:

- Isolation prevents or limits cross-talk between I/O circuits in the control system.
- Isolation prevents or limits propagation of damage caused by high amplitude transients from the point of application to other circuits or modules.

This test applies the specified level of AC and DC voltage to individual examples of each type of circuit included in the test specimen.

6.2.4.8 Post-Qualification Test

The Post-Qualification Tests consists of re-running complete Operability and Prudency tests at HFC after completion of all qualification tests. The purpose of the Post-Qualification Tests is to obtain a record of Test Specimen performance after being subjected to the complete set of qualification tests. These test results are then compared to those from the Pre-Qualification Test results to establish the overall capability of the FPU controller modules.

6.2.5 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. The test results are contained in the following reports:

- TR901-302-01, VV0115 Pre-Qualification Test Report, Rev A
- TR901-302-02, VV0115 Environmental Stress Test Report, Rev A
- TR901-302-03, VV0115 EMI RFI Test Report, Rev A
- TR901-302-04, VV0115 Surge Withstand Test Report, Rev A
- TR901-302-05, VV0115 Electrostatic Discharge Withstand Test Report, Rev A
- TR901-302-06, VV0115 Seismic Test Report, Rev A
- TR901-302-07, VV0115 Isolation Test Report, Rev A
- TR901-302-08, VV0115 Post-Qualification Test Report, Rev A

7.0 CONCLUSION

The HFC-FPU control system platform implements the functional characteristics of the HFC-6000 control system platform using FPGA architecture. The design and implementation of the HFC-FPU control 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-FPU control system qualification tests were constructed and performed in accordance with EPRI TR-107330, because the FPU-based systems are basically the same as the PLCs in terms of digital devices.

Based on the design and implementation of the HFC-FPU control system including EQ results, HFC concludes that the HFC-FPU control system 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-FPU control system platform. See Table 4.

Table 4. List of the HFC-FPGA control platform to be included in the SE

Module	P/N	Rev
FPU Controller for 16 DI Channels and 16 DO Channels	40117481	C
FPU Controller for 32 DI Channels	40117482	C
FPU Controller for 16 4- to 20-mA AI Channels	40124281	C
FPU Controller for 8 AO Channels	40129481	D
FPU Controller for 8 AI Channels for Type E Thermocouples	40127081	A
FPU Controller for 8 AI Channels for 100-Ohm Platinum RTDs	40127481	A
FPU Controller for 8 AI Channels for 100-Ohm Platinum RTDs	40145781	A
FPU CPU module	40132281	A
FPU CPU module	40145281	A
F-Link High Speed Interface Module	40108689	B