U.S. Nuclear Regulatory Commission Staff

Final Safety Evaluation for

Topical Report RR901-107-10,

"Amendment for HFC-FPGA System of HFC-6000 Safety Platform," Revision F

March 2021

Principal Contributors: Richard Stattel, Jack Zhao

List of Abbreviations

A/D	Analog-to-Digital
AC	Alternating Current
ADAMS	Agencywide Documents Access and Management System
AI	Analog Input
ANSI	American National Standards Institute
AO	Analog Output
ASME	American Society of Mechanical Engineers
ASTS	Automatic Seismic Trip System
ATWS	Anticipated Transients Without Scram
AUX	Auxiliary
BOE	Burst of Events
BOM	Bill-of-Materials
BTP	Branch Technical Position
C	Celsius/Centigrade
CCF	Common Cause Failure
CFR	Code of Federal Regulations
C-Link	Communication link between HFC-FPGA Gateways and EWS (implemented with a token-passing protocol)
CLB	Configurable Logic Block
CPLD	Complex Programmable Logic Device
CPU	Central Processing Unit
CQ4	HFC Analog Algorithm
CRC	Cyclic Redundancy Check
D/A	Digital-to-Analog
DDB	Dynamic Database
DI	Digital Input
DIP	Dual In-line Package
DO	Digital Output
EFT	Electric Fast Transient
EMI	Electro-Magnetic Interference
ELPC	Ethernet Low Pin Count Connection Interface
EPRI	Electric Power Research Institute
EPROM	Erasable Programmable Read-Only Memory
EQ	Environmental Qualification
ESD	Electrostatic Discharge
ESFAS	Engineered Safety Features Actuation System
EWS	Engineering Workstation
F-Link	FPGA Communication Link (uses token-passing protocol developed for the C-Link and backplane hardware traces developed for the Intercommunication Link)
FPC	Fast Performance Controller
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
GOI	Generic Open Item
HAS	Historical Archiving System
HDL	Hardware Description Language
HDS	Hardware Design Specification

HFC	HF Controls
HICB	Human Factors/Instrumentation and Control Branch
HPAT	HFC Programmable Automatic Tester
HPI	HFC Peripheral Interface
HRS	Hardware Requirements Specification
HSIM	High Speed Interface Module
Hz	Hertz
I&C	Instrumentation and Control
IAEA	International Atomic Energy Agency
IBR	Incorporate by Reference
ICL	Intercommunication Link
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
I/O	Input / Output
IP	Intellectual Property
JTAG	Joint Test Action Group
LAB	Logic Array Block
LWR	Light Water Reactor
Ms	millisecond
mA	milliampere
Mbps	Megabits per second
MFM	Master-for-a-Moment
MHz	Megahertz
ML	Main Library (of ADAMS)
MS	Microsoft
MSB	Most Significant Bit
NP	Non-Proprietary
NPP	Nuclear Power Plant
NQA	Nuclear Quality Assurance
NRC	United States Nuclear Regulatory Commission
NUREG	U.S. Nuclear Regulatory Commission technical report designation
OBE	Operating Basis Earthquake
OEM	Original Equipment Manufacturer
OI	Open Item
PCB	Printed Circuit Board
PI	Proprietary Information
PLC	Programmable Logic Controller
PLL	Phase Lock Loop
PS	Power Supply
PSAI	Plant Specific Action Item
QA	Quality Assurance
QAPM	Quality Assurance Program Manual
QPP	Quality Process Procedure
QTS	Qualification Test Specimen
R&D	Research & Development
RFI	Radio Frequency Interference
RG	Regulatory Guide
RH	Relative Humidity
RIF	Redundancy Interface
RPS	Reactor Protection System
RQ	Request Tables
RRS	Required Response Spectrum
RS	Recommended Standard

RTD	Resistance Temperature Detector
RTL	Register-Transfer Level
RTS	Reactor Trip System
RX	Receiver
SAR	Safety Analysis Report
SCR	System Change Request
SE	Safety Evaluation
SER	Safety Evaluation Report
SEU	Single Event Upset
SIL	Software Integrity Level
SOC	System-on-a-chip
SOE	Sequence of Events
SQL	Structured Query Language
SRP	Standard Review Plan
SRS	Software Requirement Specification
SSC	Structures, Systems and Components
SSE	Safety Shutdown Earthquake
STA	Static Timing Analysis
Std	Standard
SWC	Surge Withstand Capability
TMR	Triple Modular Redundant
TR	Topical Report
TRS	Test Response Spectrum
TSAP	Test Specimen Application Program
TUV	Technischer Überwachungsverein (Association for Technical Inspection - Germany)
TX	Transmitter
USNRC	United States Nuclear Regulatory Commission
V&V	Verification & Validation
VGA	Video Graphic Array
VHDL	VHSIC Hardware Description Language
VHSIC	Very High-Speed Integrated Circuit
V	Volts
Vrms	Voltage Root Mean Square
WI	Work Instruction

Table of Contents

FINAL SAFETY EVALUATION

BY THE OFFICE OF NUCLEAR REACTOR REGULATION

FOR HFC-FPGA SAFETY PLATFORM TOPICAL REPORT AMENDMENT 4

EPID NO. L-2016-TOP-0010

1.0 INTRODUCTION AND BACKGROUND

By letter dated April 15, 2019 (Reference 1), HF Controls Corporation (HFC), a subsidiary of Doosan Heavy Industries and Construction Company, submitted topical report (TR) RR901-107-10-PI, "Amendment for HFC-FPGA [field programmable gate array] System of HFC-6000 Safety Platform," Revision F (References 2 & 3) for review and acceptance by U.S. Nuclear Regulatory Commission (NRC) staff. HFC is seeking the NRC's generic approval of its current generation of the HFC-FPGA safety platform, which is based on FPGA technology.

The microprocessor technology-based HFC-6000 safety platform was previously submitted (Reference 4), evaluated, and approved by the NRC staff for use in nuclear power plant (NPP) safety-related applications, as PP901-000-01CF-P/NP-A (Reference 5). This previous HFC 6000 platform TR SE contained several generic open items (GOIs). HFC subsequentially submitted additional information related to the HFC-6000 safety platform to close out six GOIs (Reference 6). In a letter dated March 4, 2015, the NRC staff issued a safety evaluation (SE) (Reference 7) to close out those six GOIs.

The NRC staff performed an acceptance review of the HFC-FPGA safety platform TR Amendment 4 and found that the material submitted was sufficient to begin a detailed technical review (Reference 8).

The NRC staff submitted Requests for Additional Information (RAIs) (Reference 11) to obtain information needed to complete this SE. HFC provided the responses to these RAIs in Reference 14.

The NRC staff conducted a virtual audit of HFC in May of 2020 in accordance with Office of Nuclear Reactor Regulation Office Instruction LIC-111, "Regulatory Audits" (Agencywide Document Access and Management System Accession No.: ML082900195). An audit plan (Reference 12) was prepared to define audit activities to be performed. The purpose of this audit was to verify the effectiveness of the HFC logic development activities and to confirm that processes described in the TR are being effectively implemented to achieve a high-quality system that can be used to perform safety-related functions in a nuclear facility. The results of the audit are documented in the "Regulator Audit Report for the HFC-FPGA Digital FPGA Platform Licensing Topical Report" (Reference 13).

The scope of this SE of the FPGA based HFC-FPGA platform includes the development and test plans, specifications and procedures used to design, and perform verification and validation (V&V) of the standardized HFC-FPGA circuit boards described in the TR. This SE scope also includes the safety lifecycle processes to be used for development of HFC-FPGA plant-specific logic. This SE scope excludes evaluation of the integration and testing of plant specific system applications, factory acceptance test of plant systems, or maintenance activities to support installed plant systems.

2.0 REGULATORY EVALUATION

The purpose of this SE is to document the NRC staff evaluation of whether the HFC-FPGA platform is suitable for use in safety-related applications. Thus, the review of the TR and supporting technical documents is intended to determine whether sufficient evidence is presented to enable a determination with reasonable assurance that subsequent applications based on the HFC-FPGA platform can comply with the applicable regulations to ensure that the public health and safety will be protected.

The NRC staff used NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," Revision 7, to conduct this evaluation. NUREG-0800, which is hereafter referred to as the Standard Review Plan (SRP), sets forth a method for reviewing compliance with applicable sections of Title 10 of the Code of Federal Regulations (10 CFR) Part 50, "Domestic Licensing of Production and Utilization Facilities" and 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants." Specifically, SRP Chapter 7, "Instrumentation and Controls," addresses the requirements for instrumentation and control (I&C) systems in NPPs based on light-water reactor designs. The procedures for review of digital systems applied in this evaluation are principally contained within SRP Chapter 7 and are supplemented by interim staff guidance (ISG).

The suitability of a digital I&C platform for use in safety systems depends on the quality of its components; quality of the design process; and its environmental qualification (EQ), along with consideration of system implementation characteristics such as real-time performance, independence, and support of on-line surveillance requirements as demonstrated through the digital I&C platform's verification, validation, and qualification efforts. Because HFC-FPGA equipment is intended for use in safety-related systems and applications, the platform TR was evaluated for compliance with the criteria of Institute of Electrical and Electronics Engineers (IEEE) Standard (Std.) 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" and SRP Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603." The HFC-FPGA platform TR was similarly evaluated against the criteria of IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," and Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2."

Determination of compliance with applicable regulations remains subject to a plant-specific licensing review of a complete system design based on the HFC-FPGA platform. GOIs and plant specific action items (PSAIs) are established in Section 5 of this SE, "Limitations and Conditions" to identify criteria to be addressed by an applicant or licensee referencing this SE. These criteria are provided to facilitate an applicant's or licensee's ability to establish compliance with applicable plant design criteria and regulations identified in SRP Chapter 7, Table 7-1. The PSAIs identified in Section 5.2 do not obviate an applicant's or licensee's responsibility to address new or changed design criteria or regulations that apply in addition to those used to perform this SE when making changes to its facility.

The following regulations are applicable to the HFC-FPGA platform TR:

- 10 CFR 50.54 (jj) and 10 CFR 50.55(i), Require that structures, systems, and components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed
- 10 CFR 50.55a(h), "Protection and Safety Systems" incorporates the 1991 version of IEEE Std. 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power

Generating Stations," by reference, including the correction sheet dated January 30, 1995

- 10 CFR Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants"
  - GDC 1, "Quality Standards and Records"
  - GDC 2, "Design Bases for Protection Against Natural Phenomena"
  - GDC 4, "Environmental and Dynamic Effects Bases"
  - GDC 13, "Instrumentation and Control"
  - GDC 20, "Protection System Functions"
  - GDC 21, "Protection System Reliability and Testability"
  - GDC 22, "Protection System Independence"
  - GDC 23, "Protection System Failure Modes"
  - GDC 24, "Separation of Protection and Control Systems"
  - GDC 25, "Protection System Requirements for Reactivity Control Malfunctions"
  - GDC 29, "Protection Against Anticipated Operational Occurrences"
- 10 CFR Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants"
- 10 CFR Part 21, "Reporting of Defects and Noncompliance"

The NRC staff used the applicable portions of the guidance provided in the following regulatory guides (RG) and the digital instrumentation and control (DI&C) interim staff guidance (ISG):

- RG 1.22, "Periodic Testing of Protection System Actuation Functions," Revision 0
- RG 1.28, "Quality Assurance Program Criteria (Design and Construction)," Revision 5
- RG 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems," Revision 1
- RG 1.53, "Application of the Single-Failure Criterion to Safety Systems," Revision 2
- RG 1.62, "Manual Initiation of Protective Actions," Revision 1
- RG 1.75, "Criteria for Independence of Electrical Systems," Revision 3
- RG 1.100, "Seismic Qualification of Electrical and Active Mechanical Equipment and Functional Qualification of Active Mechanical Equipment for Nuclear Power Plants," Revision 3
- RG 1.105, "Setpoints for safety-Related Instrumentation," Revision 3
- RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Revision 3.
- RG 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 2
- RG 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 1
- RG 1.170, "Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 1
- RG 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 1
- RG 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 1
- RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 1
- RG 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-Related Instrumentation and Control Systems," Revision 1
- RG 1.209, "Guidelines for Environmental Qualification of safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants," Revision 0

- DI&C-ISG-04, “Task Working Group #4: Highly-Integrated Control Rooms—Communications Issues (HICRc),” Revision 1
- DI&C-ISG-06, “Licensing Process,” Revision 2

The NRC staff used the following NRC Technical Reports to support this evaluation:

- NUREG-0800, “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants”
- NUREG/CR-6101, “Software Reliability and Safety in Nuclear Reactor Protection Systems”
- NUREG/CR-6303, “Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems”

The NRC staff also used applicable portions of the guidance listed in the following SRP Chapter 7 branch technical positions (BTP):

- BTP 7-11, “Guidance on Application and Qualification of Isolation Devices,” Revision 6
- BTP 7-14, “Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems,” Revision 6
- BTP 7-17, “Guidance on Self-test and Surveillance Test Provisions,” Revision 6
- BTP 7-18, “Guidance on Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems,” Revision 6
- BTP 7-19, “Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems,” Revision 7
- BTP 7-21, “Guidance on Digital Computer Real-Time Performance,” Revision 6

The following industry guidance documents were also used to perform this evaluation.

- IEEE Std. 7-4.3.2-2003, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations”
- IEEE Std. 323-2003, “IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations”
- IEEE Std. 344-2004, “IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations”
- IEEE Std. 352-1987, “IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems”
- IEEE Std. 379-2000, “IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems”
- IEEE Std. 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations”
- IEEE Std. 828-2005, “IEEE Standard for Configuration Management Plans”
- IEEE Std. 829-2008, “Test Documentation”
- IEEE Std. 830-1998, "IEEE Recommended Practice for Software Requirements Specifications”
- IEEE Std. 1008-1987, “Software Unit Testing”
- IEEE Std. 1012-2004, “IEEE Standard for Software Verification and Validation”
- IEEE Std. 1074-2006, “IEEE Standard for Developing a Software Project Life Cycle Process”
- Electric Power Research Institute (EPRI) Topical Report (TR)-102323, "Guidelines for Electromagnetic Interference Testing in Power Plants," as accepted by the NRC staff SE dated April 30, 1996

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

3.0 TECHNICAL EVALUATION

The following subsections describe the HFC-FPGA platform's components and the processes used to develop them. These sections also include evaluations of these components against the regulatory evaluation criteria identified in Section 2.0 of this SE.

3.1 System Background

The HFC-FPGA platform is based upon FPGA-based technology rather than microprocessors and complex programmable logic devices (CPLDs) as was the case in previous HFC-6000 version of this platform. See Reference 5. The HFC-FPGA platform is not intended to replace the microprocessor based HFC-6000 platform. Instead, the HFC-FPGA platform is intended to provide the same capabilities as the original HFC-6000 platform using a different hardware, software and logic configurations. As such, HFC can provide both FPGA and microprocessor-based solutions as a means of addressing diversity of a protection system design. This diversity aspect is not being addressed in this evaluation and must instead be assessed at the plant level during plant application development. See PSAIs in Section 5.2.13 of this SE for additional information on these activities.

3.2 System Description

The HFC-FPGA platform is a digital I&C system that can be used to perform a wide variety of safety-related functions, such as reactor trip or engineered safety features actuation functions, in a NPP. The HFC-FPGA platform is comprised of an equipment chassis, power supplies, controller modules, input/output (I/O) modules and various communication interfaces that can be used to support both intra-communication within the division and inter-divisional communication with devices external to the safety division.

All modules of the HFC-FPGA platform are designed using FPGA-based technology except for the Gateway Controller, designated as HFC-FPC-08, which is based on microprocessor technology.

The HFC-FPGA platform is comprised of modules and supporting components, which are listed in Tables 3.2-1 and 3.2-2 of this SE. The HFC-FPGA platform modules consist of seven types of I/O modules, two types of controller modules and two types of communication modules. The scope of the review is limited to those modules and components that would exist within in a single division of a safety system. Changes to platform components, development processes, and logic configurations made subsequent to completion of this SE will need to be addressed as a plant specific action item. See PSAI 5.2.1.

Table 3.2-1 HFC-FPGA Platform Qualified Module List

Module Type	Part Number	Module Name	Description
HFC Chassis	Controller / Expansion Backplane	70070902 F	HFC 6000 Expansion Chassis Standard
Input / Output	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 (designed for a higher input accuracy)
Controller	40132221Q	HFC-FCPU	FPGA Controller Module for the HFC-FPGA system with onboard I/O function
	40145221Q	HFC-FCPUX	FPGA Controller Module for the HFC-FPGA System
Communication	40108621Q	HFC-HSIM	F-Link High Speed Interface Module
	40103834Q	HFC-FPC08	Communication Gateway Controller Without VGA

Table 3.2-2 HFC-FPGA Auxiliary Components List	
Part Number	**Description**
9044514	PS, 8-SLOT RACK (40MS HOLD-UP) HML
9044517	P/S FILLER PLATES HML601 6.4"H JASPER HML601 6.4"H
9044526	M1238 Rack Standoff
9044524	PS, JASPER 24V (40MS HOLD-UP)
7868303	CONNECT PLUG MOLEX 03-06-2061
7885502	CONT MOLEX 02-06-2103 .06 DIA
70070902	HFC 6000 EXPANSION CHASSIS STANDARD
6990176	FAN TRAY, 24VDC, NORVELL
6990318	CONN, MOLEX SOCKET
6990319	PIN, MOLEX
7151601	C/B, IC 10000A @240VAC GE TEB
7648600	CONNECTOR ITE LN1-E100
7066201	TERMINAL BLOCK, KULKA 672-12P
7077187	EMI FILTER, 250VAC, 20A TDK-LAMBDA P/N: RSHN-2020
S931201Q	SURGE ARREST PHX CNTCT - PT 2-PE/S-120AC-ST
S931202Q	SURGE ARRESTOR SOCKET PHOENIX CONTACT - PT-BE/FM
7845050	WM 38356 END BRACKET (EW 35)
7066000	TERMINAL BLOCK, KULKA 672-6
70056201	BUS BAR ASSY INSTRUMENT GROUND
7663704	FUSEHLDR,4 POLE BLOCK 359 004
40129881Q	PCB ASSY HFC-TBDO16T4
71003902Q	TERMINAL BOARD INSULATION SHEET, 3.5" x 13.8"
71002409Q	CABLE ASSEMBLY, DB50, 9 FOOT S10097, TYPE A
40130681Q	PCB ASSY HFC-TBDI16T3
71003901Q	TERMINAL BOARD INSULATION SHEET, 3.5" x 8.5"
40135881Q	PCB ASSY HFC-TBAI8LT
40141081Q	PCB ASSEMBLY HFC-TBAI8MT
70082309Q	CABLE ASSEMBLY, DB25, 9 FOOT S10096, TYPE A
40133081Q	PCB ASSY HFC-TBAO8T
40117082Q	HFC-TBAI16T WITH BUSBAR ASSY
70047001	CABLE ASSY FIBER OPTIC BLACK CABLE ASSY FIBER OPTIC BLACK
9049920	CABLE, CAT5e, RED 6 FEET STRAIGHT PINNED, SNAGLESS BOOT
9049982	CABLE, CAT5e, YELLOW 6 FEET STRAIGHT PINNED, SNAGLESS BOOT

Table 3.2-2 HFC-FPGA Auxiliary Components List	
Part Number	**Description**
9049934	CABLE, CAT5E, BLUE 6 FEET STRAIGHT PINNED, SNAGLESS BOOT
9049981	CABLE, CAT5e, GRAY 6 FEET STRAIGHT PINNED, SNAGLESS BOOT
71004202Q	CAT6A GIGABIT CROSSOVER CABLE SHIELDED, TIA/EIA 568B
40103834Q	PCB & BEZEL ASSY, HFC-FPC08 GLINK
40145221Q	PCB & BEZEL ASSY, HFC-FCPUX
40132221Q	PCB & BEZEL ASSY, HFC-FCPU
40124221Q	PCB & BEZEL ASSY, HFC-FPUA01
40117421Q	PCB & BEZEL ASSY, HFC-FPUD01 16 DI/16 DO
40117422Q	PCB & BEZEL ASSY, HFC-FPUD02 32 DI
40108621Q	PCB & BEZEL ASSY, HFC-HSIM
40129421Q	PCB & BEZEL ASSY, HFC-FPUAO
40127021Q	PCB & BEZEL ASSY, HFC-FPUL
40127421Q	PCB & BEZEL ASSY, HFC-FPUM
70071102Q	HFC 6000 BEZEL ASSEMBLY, BLANK SINGLE BLANK
40123081Q	HFC-FPC08CON4 ASSEMBLY
40129081Q	PCB ASSY HFC-FPUDCON

The auxiliary components are HFC-FPGA platform components that were included in the equipment under test during platform qualification testing. These components, though not individually evaluated by the NRC staff, were confirmed to be included in the platform test configuration and are accepted by the NRC for use in nuclear safety-related applications.

3.2.1 HFC-FPGA Digital I&C Platform Central Controller Architecture and Platform Modules

The HFC-FPGA platform can be implemented using one of three design architectures described in the TR. However, for the purposes of safety-related nuclear applications, only one of these possible architectures, the central controller architecture, is being evaluated in this SE. Within this architecture, a redundant pair of FPGA-based controller modules are linked to FPGA-based I/O modules, thus enabling the configuration to serve in an ‘input, processing and output’ capacity. The applicant intends to use the resulting configuration as an autonomous controller with I/O modules that serve as part of a single safety train or division within a safety-related NPP DI&C application. Implementations of architectures other than central controller are not approved for use in nuclear safety applications. The following subsections provide general functional descriptions for the HFC-FPGA platform modules.

3.2.1.1 Input Output Modules

The seven I/O modules listed in Table 3.2-1 provide the hardware interface to field sensors and control field devices and are implemented by different types of I/O printed circuit boards (PCBs). The I/O modules communicate with the controller module(s) via redundant RS-485 traces on the

backplane of the HFC-6000 rack using HFC proprietary token-passing protocol originally developed for the C-Link. This communication link is designated as F-Link.
As with the modules from the original HFC-6000 platform, all modules in the HFC-FPGA platform, except the Gateway controller HFC-FPC08, communicate with plant equipment via I/O module interfaces. Different versions of I/O modules provide various types of interfaces with field equipment, such as 4 – 20 Milliampere (mA) direct current (DC) signal inputs and outputs, resistance temperature detector (RTD) inputs, and digital inputs (DI) and digital outputs (DO). (Refer to Table 3.2-1 for available I/O module types)

3.2.1.1.1 Digital Input and Output Modules

The HFC-FPUD type module is a 32-channel DI and digital output DO module. The HFC-FPUD01 module has 16 DI channels and 16 Form C Relay DO channels. The HFC-FPUD02 supports 32 DI channels. Additional information on the HFC-FPUD modules can be found in Section 5.1.2.2.1 of the HFC-FPGATR (References 2 and 3).

3.2.1.1.2 Analog Input Module

The HFC-FPUA01 module is an analog input (AI) module designed to support 16 isolated AI channels. The HFC-FPUA01 is designed to process 4-20 mA dc AI signals using an FPGA-based 24-bit Analog-to-Digital (A/D) converter with advanced signal conditioning. These 16 channels can be configured for either self-powered or transmitter-powered operation. Additional information on the HFC-FPUA01 module can be found in Section 5.1.2.2.2 of the TR (References 2 and 3).

3.2.1.1.3 Analog Output Module

The HFC-FPUAO Module is an analog output (AO) module designed to support 8 isolated AO channels. These channels operate in the range of 4-20 mA dc. The HFC-FPUAO uses a 12-bit digital-to-analog (D/A) converter with advanced signal conditioning. Additional information on the HFC-FPUAO module can be found in Section 5.1.2.2.3 of the TR (References 2 and 3).

3.2.1.1.4 Analog Input Module (for Type E Thermocouples)

The HFC-FPUL Module is an analog input module designed to support 8 isolated thermocouple AI channels plus one cold junction channel. The HFC-FPUL is designed to process Type E thermocouple signals using a 24-bit A/D converter with advanced signal conditioning. Additional information on the HFC-FPUL module can be found in Section 5.1.2.2.4 of the TR (References 2 and 3).

3.2.1.1.5 Resistance Temperature Detector Module (100 Ohm Platinum RTDs)

The HFC-FPUM and HFC-FPUM2 modules are precision RTD-measuring modules designed to support 8 RTD input channels. These RTD input channels support three different temperature ranges. Additional information on the HFC-FPUM and HFC-FPUM2 modules can be found in Section 5.1.2.2.5 of the TR (References 2 and 3).

3.2.1.2 Controller Modules

Two types of system controllers, designated as HFC-FCPU and HFC-FCPUX, support the execution of the FPGA application logic, I/O scan cycles and communication with Gateway

controller. A redundant configuration of system controllers includes two HFC-FCPU or two HFC-FCPUX controller boards which communicate with each other via an interface called Redundancy Interface (RIF). The given application-specific layout determines if one or both types of controllers will be used in a safety system or division. For the purposes of this evaluation, the platform layout consists of two redundant FPGA-based controllers being linked to HFC-FPGA I/O modules and communication modules. This layout is designated by HFC as the *"central controller"* architecture.

The principal functions performed by a controller module are:

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

Both HFC-FCPU and HFCFCPUX use FPGA chips to perform the overall operating function of the system. The major differences between these two system controllers are that HFC-FCPUX module is designed to support a larger capacity FPGA chip and it does not have onboard DI/DO channels, while there are eight DI channels and eight DO channels in the HFC-FCPU.
The DI and DO channels on HFC-FCPU are present in the design of the given FPGA however, HFC is imposing a requirement that digital I/O functions in HFC-FCPU will be disabled such that controller DI and DO channels will not be used in nuclear safety system applications. Therefore, the controller DI and DO functionality is not evaluated in this SE. This constraint is being applied to safety-related applications of the system controllers to avoid introduction of non-qualified interfaces. This is GOI 5.1.1.

Additionally, the larger capacity FPGA chip in HFC-FCPUX will not use its additional processing capacity, when compared to its HFC-FCPU counterpart, in a manner that surpasses the HFC-FCPU's ability to process an application used within the HFC-FCPU as system controller. The HFC-FCPUX and the HFC-FPCU are therefore interchangeable. For this evaluation, the two FPGA module types are treated as identical in function and operation as centralized controller modules.

3.2.1.3 Gateway Module

The Gateway Module HFC-FPC08 is a communications controller. It broadcasts the necessary operation status to external devices via the C-Link network. The Gateway controller also receives and transmits data from the controller module redundant pairs (HFC-FCPU or HFC-FCPUX) via a network designated as the G-Link. G-Link communication is implemented via the redundant RS-485 traces on the backplane of the chassis using the HFC proprietary token-passing C-Link protocol.

3.2.1.4 High Speed Interface Module (F-Link)

The High-Speed Interface Module (HSIM) is designed to be used as an information carrier for other portions of the system. It is configured with optical transmission and reception ports and may be used with the F-Link and Intercommunication Link (ICL) communication protocols and supports communication with a fiber optic network.

The F-Link is a communication pathway that provides communications between controller modules and the systems I/O modules. There are two redundant paths in the F-Link. In some system configurations where an expansion rack is used or another device needs to have its signal processed by the system controller, the HSIM module can be used to support F-Link communication with these devices.

Note: In the SE of the HFC-6000 platform (Reference 5), the function of passing information between the I/O modules and the controllers was performed by an ICL. The ICL uses a master/slave protocol which does not apply to the HFC-FPGA platform under review.

3.2.2 Hardware Composition of Modules

All HFC-FPGA module assemblies, except for the HFC-FPC08 Gateway module, include the following hardware components and use the HFC-6000 form factor and connector arrangement from earlier versions of the system such that the PCB on which the hardware resides is compatible with earlier versions of the HFC-6000 platform:

- FPGAs - Two FPGA modules are located on module's PCB and communicate with one another via an HFC Peripheral Interface (HPI) link
- Memory - Flash memory for each FPGA is provided which provides non-volatile storage for configuration parameters
- Voltage Regulators - Two complete sets of switching voltage regulators produce all required onboard voltage levels
- Voltage Monitoring - There are separate voltage monitors for each of the two power rails
- Communication - Redundant RS-485 transceivers constitute the hardware interface to the F-Link
- Station (Physical Location) Interface - The Station ID interface enables the FPGAs to read the Station ID number from the hardwired slot location-based code on the backplane
- Maintenance/Run Switch - Maintenance/Run switch enables manual selection between offline maintenance and normal run modes of operation for the FPGA Controllers
- Reset Switch - The reset switch enables manual reset of the assembly
- Light-Emitting Diode (LED) Indicators - Board-edge LEDs provide a visual indication of PCB operating status for communication, input/output channel status, and error codes

Section 5.1.1 of the HFC TR provides descriptions and additional information for each of these common hardware components of the HFC-FPGA module assemblies.

3.2.3 HFC-FPGA Platform Communications

The HFC-FPGA platform includes interfaces to support both internal and external communications. Internal communication interfaces are used to establish data communication pathways between system modules and components that are all within a single safety division.

There are four internal interfaces used in the HFC-FPGA platform as follows:

- F-Link - Used for communications between controller modules and I/O modules in the system and for extension of I/O to additional chassis through an HSIM.
- G-Link – Used for communications between controller modules and the gateway controller module.
- Redundancy Interface - The RIF is a serial communication interface between the redundant HFC-FCPU modules. The RIF interface provides a means of keeping the

secondary HFC-FCPU module updated with a current copy of the primary HFC-FCPU running status.

- HFC Peripheral Interface – Communications between the controller FPGA and the Diagnostic FPGA are conducted through an HPI Peripheral Interface (HPI) link. The HPI link provides a means of communicating diagnostic data between the Control FPGA and the Diagnostic FPGA within a Controller Module. HPI interfaces do not extend to the chassis backplane and are therefore physically isolated to a single module.

External communication interfaces are used to establish a uni-directional communication pathway to devices that are external to the safety division. The C-Link interface is used for HFC-FPGA external communications to non safety-related systems.

3.2.4 Use of Intellectual Property Cores in HFC-FPGA Platform Design

Intellectual Property (IP) Cores are used in HFC-FPGA design. These are blocks of FPGA logic that are not developed by HFC but are configured and used for HFC-FPGA product development. The vendor-specific IP cores used in the HFC-FPGA system are discussed in Section 5.3 of the HFC-FPGA platform TR. Design specification DS001-007-02, "HFC-6000 FPGA System IP Core Design Description," includes a list of IP cores used and their descriptions.

These IP cores were evaluated during the platform V&V process. Based on the HFC evaluation of DS001-007-02, these cores were found to be suitable for use in the HFC-FPGA system.

To verify this HFC conclusion, the NRC staff reviewed DS001-007-02 as part of its virtual audit. This review found that the HFC-FPGA platform does not use soft core IP blocks. Soft core IP blocks are logic that is developed by a third-party vendor which can be modified by the user for specialized use. The system does however make use of several configurable hard-core blocks. These blocks are used in the internal architecture of the platforms' FPGA devices and have been analyzed by HFC for use. The NRC staff also confirmed that functions of these IP core blocks have been verified by HFC verification and validation (V&V) activities performed on system outputs in accordance with method b) of IEEE Std. 7-4.3.2-2003 Clause 5.3.2. The use of configurable hard-core blocks in the HFC-FPGA platform is therefore acceptable.

3.3 HFC-FPGA Platform Development Processes

The development processes used by HFC for the HFC-6000 platform remain relevant and applicable to development activities associated with the HFC-FPGA platform. These processes were evaluated by the NRC staff during the HFC-6000 platform evaluation and, to the extent possible due to the limitations of the generic platform review, were found to be acceptable (Reference 5). The NRC staff determined that many of the development processes used by HFC exhibit the functional and process characteristics identified in SRP BTP 7-14 necessary to provide adequate evidence of quality software for use in nuclear safety applications.
The overall HFC-FPGA platform development lifecycle is described in Sections 5.4, "FPGA Software Development Process," and 5.5, "FPGA specific implementation" of the HFC-FPGA platform TR (References 2 & 3). This lifecycle is used for both hardware development activities and FPGA technology specific development activities. HFC-FPGA module application logic development processes are described in Section 5.6, "Application Control" of the HFC-FPGA platform TR.

The HFC-FPGA platform development processes include technical processes for platform hardware, software, and system design. Each of these technical processes consists of a series of phases that include development activities necessary to produce an integrated platform system. The phases of these technical processes are described in Section 5.4 of the HFC-FPGA platform TR and are illustrated in Figure 15 of that report.

FPGA design and programing are part of the system implementation process in the overall I&C system design. The FPGAs in the HFC-FPGA platform are developed using a defined lifecycle process that is comparable to the lifecycle processes described in IEEE 1012-2004. The HFC-FPGA platform development lifecycle includes requirements, design, implementation, integration, and test phases.

HFC has revised these processes to accommodate technology specific activities associated with FPGA design development. These revised processes are described in Section 5.5 of the HFC-FPGA platform TR. The NRC staff evaluated these changes and determined the revised processes provide an acceptable means of producing a system for use in nuclear safety applications. Licensees referencing this TR should conduct vendor oversite activities to ensure that HFC performs development activities in accordance with these acceptable processes. This is PSAI 5.2.2

3.3.1 HFC-FPGA Logic and Software Development Lifecycle Process Planning

With the exception of the HFC-PFC08 module, the HFC-FPGA platform does not use software during operation. It does however use programmable logic that is based on a hardware descriptive language that is similar to the instruction-based languages used in software systems. The NRC staff considers guidance for software planning and development to be applicable to the processes used for FPGA and CPLD logic development. The following sections describe and evaluate the planning aspects of HFC-FPGA platform logic and software development.

3.3.1.1 Management Planning

Criteria used to evaluate HFC-FPGA management planning was derived from the following:

- BTP 7-14, Section B.3.1.1, “Acceptance Criteria for Software Management Plan”
- RG 1.173, “Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants”
- IEEE Std. 1074-2006, "IEEE Standard for Developing Software Life Cycle Processes", Chapter 3, "Project Management Process."

Management aspects of HFC-FPGA platform software and logic development process are described in Sections 5.4, “FPGA Software Development Process” of the HFC-FPGA platform TR. HFC functional teams include an engineering development team, an independent V&V team, and a quality assurance (QA) group. The roles and responsibilities for each of these teams is defined within the companies’ work instructions. During the HFC-FPGA virtual audit, the NRC staff reviewed several HFC work instructions and confirmed these documents contained guidance for assigning roles and responsibilities for associated work activities.

For example, the requirements traceability verification procedure assigns the V&V team, or independent reviewer as being responsible for the creation of the requirements matrix.
The HFC QA department that is separate from the other departments responsible for a project is responsible for QA management and V&V oversight. A QA manager and a V&V team are

assigned for each project. The QA manager is responsible for overseeing QA activities and the V&V team performs independent evaluation of the processes and products for a software lifecycle implementation.

The NRC staff observed that HFC work instructions demonstrate adequate organization and authority structure for the HFC-FPGA platform design, procedures, and the relationships between different development activities. Furthermore, the NRC staff determined the management structure described in the HFC-FPGA platform TR, Sections 5.4, and 5.5 provide for adequate project oversight, control, reporting, review, and assessment of platform component design. The NRC staff concludes that HFC meets the requirements for management planning outlined in IEEE Std. 1074-2006 as endorsed by RG. 1.173 and is therefore, acceptable.

3.3.1.2 Development Planning

Section B.3.1.2, "Software Development Plan" of BTP 7-14 was used for evaluation of HFC-FPGA development planning.

HFC-FPGA system is specifically developed for nuclear applications and therefore is not considered commercial grade digital equipment. HFC-FPGA development process is described in Sections 5.4, "FPGA Software Development Process" of the HFC-FPGA platform TR.

HFC-FPGA Logic Development Process

Configurable Logic Blocks (CLBs) are used for implementation of logic in the HFC-FPGA platform and therefore the term Logic is synonymous with CLB for the purposes of this discussion. HFC development teams develop CLBs for the HFC-FPGA modules that are then used to implement plant-specific instrumentation protection and control logic functions. A CLB consists of set of FPGA configuration files that are installed into the HFC-FPGA Modules. The HFC logic development lifecycle is described in Section 5.4, "FPGA Software Development Process" of the HFC-FPGA platform TR. This lifecycle consists of the following phases.

- Concept Development and System to SW Allocation
- Software Requirements
- Analysis
- Software Architectural Design
- Software Detailed Design
- Software Construction
- Software Integration
- Software Qualification
- Software Acceptance
- Software Installation

These lifecycle phases are consistent with a classic waterfall model like the model discussed in Section 2.3.1 of NUREG/CR-6101. FPGA architecture and detailed design are developed based on the FPGA Requirement Specifications. Each of the HFC-FPGA modules undergoes a separate development lifecycle. Thus, separate module specific sets of lifecycle documentation are generated to support overall HFC-FPGA platform development process.

To implement FPGA requirements, designers use a Hardware Description Language (HDL) or a schematic design. A synthesis process is then performed translate the HDL or schematic design to logic gates, memory units, registers and connections. A netlist is generated which can

then be implemented on the FPGA using a development tool. Translation, map and place-and-route processes are all performed by this tool.

The model used for HFC logic development assumes that each phase of the lifecycle is completed in sequential order from concept to the software installation phase. The NRC staff finds the HFC choice of a development lifecycle acceptable because the waterfall model is well suited for projects with known and stable requirements and where few changes to requirements are anticipated. Since HFC selected an acceptable development lifecycle model, the guidance criteria of IEEE Std. 1074-2006, Clause 2.4 has been satisfied.

HFC Logic Integrity Scheme

All HFC-FPGA modules are classified as new products with integrity level 4 as defined in IEEE Std. 1012-2004. Development of these modules follows the lifecycle process described in Section 5.4 of this SE. Because no other classes of logic are included in the HFC-FPGA platform, no graded software / logic integrity level scheme is specified for platform development. The NRC staff confirmed that HFC-FPGA platform logic development V&V activities are performed to the equivalent of Safety Integrity Level (SIL) 4 requirements as defined in IEEE 1012-2004 and finds the integrity level approach used for the HFC-FPGA platform acceptable.

3.3.1.3 Quality Assurance Planning

Criteria used to evaluate HFC-FPGA QA planning was derived from the following:

- 10 CFR Part 50, Appendix B,
- RG 1.28,
- RG 1.152,
- RG 1.173,
- BTP 7-14, Section B.3.1.3, “Software Quality Assurance Plan (SQAP)”
- IEEE Std. 7-4.3.2-2003, Clause 5.3, “Quality”
- NUREG/CR-6101, "Software Reliability and Safety in Nuclear Reactor Protection Systems," Section 3.1.2, "Software QA Plan," and Section 4.1.2, "Software QA Plan."

The HFC QA program manual (QAPM) defines the QA program for HFC products and their constituent hardware and software components. It is designed to comply with NQA-1b-2011 Addenda to ASME NQA-1-2008, NQA-1-2012, and NQA-1-2015, “Quality Assurance Requirements for Nuclear Facility Applications,” including the exceptions and clarifications identified in RG 1.28 Revision 5, Section C and 10 CFR Part 50, Appendix B. The HFC QA program is implemented through quality procedures, quality plans, work instructions, and process control sheets.

Specific elements of the QAPM address organization, the scope and management of the QA program, requirements and mechanisms for control of products, resources and processes, provisions for inspections, audits, and corrective actions. Each element of the QAPM identifies the implementing procedures, which in turn establish the basis for planning and execution of QA activities, provide forms and checklists, and identify relevant work instructions.

During the regulatory audit, the NRC staff reviewed several HFC QA procedures and work instructions. The NRC staff also interviewed HFC personnel to assess the QA program effectiveness. The NRC staff reviewed work instructions for change control, HFC change

evaluation process, and configuration item identification. The results of the NRC regulatory audit are documented in Reference 13.

The NRC staff found the organization of the HFC QA department, as described in Section 6.8 of the HFC-FPGA platform TR, has sufficient authority and organizational freedom, including sufficient independence from cost and schedule to ensure that the effectiveness of the QA organization is not compromised.

The HFC QAPM and its associated quality process procedures provide measures to ensure that logic development and maintenance activities for the HFC-FPGA platform maintain an acceptable degree of quality. Based on the review of the QA processes and procedures identified in the QAPM, the NRC staff determined the QAPM and the associated quality procedures are acceptable for maintaining FPGA logic for use in safety-related systems in NPPs.

3.3.1.4 Integration Planning

Criteria used to evaluate HFC-FPGA integration planning was derived from the following:

- RG 1.173
- BTP 7-14, Section B.3.1.4
- IEEE Std. 1074-2006, Clause A. 1.2.8, “Plan Integration”
- NUREG/CR-6101, Sections 3.1.7 & 4.1.7, "Software Integration Plan"

Sections 5.4, “FPGA Software Development Process,” and 5.5, “FPGA Specific Implementation” of the HFC-FPGA platform TR describe the integration activities that are performed during system product line and application development. Activities include integration of software, FPGA logic, and hardware as well as integration of all HFC-FPGA platform components at the system level.

The NRC staff determined the HFC integration processes provide an acceptable method for performing product integration activities needed for safety-related digital I&C system development. The HFC integration activities establish coordination with the test plans and address the use of tools, techniques, and methodologies needed to perform integration activities for HFC-FPGA platform components.

In addition to HFC-FPGA platform component integration activities, there are plant application specific integration activities that must be performed to support overall system level development and implementation. See PSAI 5.2.2 for oversight activities to be performed during application software and logic development.

3.3.1.5 Safety Planning

Criteria used to evaluate HFC-FPGA safety planning was derived from the following:

- RG 1.173, Section C.3, “Software Safety Analyses”
- SRP, BTP 7-14, Sections B.3.1.9, “Software Safety Plan (SSP)” and B.3.2.1, “Acceptance Criteria for Safety Analysis Activities”
- NUREG/CR-6101, Sections 3.1.5, and 4.1.5, “Software Safety Plan”

The HFC-FPGA platform TR states that system design includes aspects of software safety management, software safety analyses, and post development which include training, installation, startup and transition, operations support, monitoring maintenance, and retirement. HFC developed a software safety plan that defines reviews, analyses, and evaluations to be included as V&V activities to ensure safety is addressed in the design and development of a safety-related system.

Although HFC does not have a dedicated software safety team and there is not a specific individual dedicated as a safety officer, the responsibility for ensuring that software safety concerns are adequately addressed is assigned to the project manager. Organizational roles and responsibilities for software safety within the framework of a development project are to be designated in an HFC project specific safety plan. The V&V team is responsible for executing and overseeing activities focused on software and FPGA logic safety. A hazard analysis is required for both application and operating software and software safety analyses are mandated at the completion of each lifecycle phase for safety-related software and FPGA logic components.

Safety analyses activities include requirements analysis, design analysis, code analysis, safety test analysis, and change analysis. The safety design analysis for operating software and FPGA logic addresses functionality of the platform and considers safety design characteristics that have been incorporated into the system. The safety code analysis for platform modules addresses traceability, internal logic, interface support, and coding style while the safety test analysis encompasses component and module testing as well as system integration and functional testing. The safety change analysis involves assessment of the safety impact of changes to platform modules or the design for the system under development.

The HFC corrective action processes are used to address corrective actions for conditions adverse to quality. This corrective action process includes provisions for documenting safety concerns and for initiating actions to address these concerns. Corrective action processes and associated documentation were reviewed during the regulatory audit and were found to effectively address issues and adverse conditions identified throughout the product lifecycle.

The NRC staff found that HFC safety lifecycle documentation shows that system safety requirements have been adequately addressed for defined safety lifecycle activities. The NRC staff determined that safety planning for platform components is acceptable for HFC-FPGA based safety systems. Furthermore, the NRC staff observed during the regulatory audit, that HFC-FPGA product safety planning provides adequate assurance that safety activities will be effective in resolving safety issues presented during the design and development of an HFC-FPGA platform-based safety system.

3.3.1.6 Verification and Validation Planning

Criteria used to evaluate HFC-FPGA V&V planning was derived from the following:

- RG 1.168
- SRP BTP 7-14, Section B.3.1.10, “Software V&V Plan (SVVP)”
- IEEE Std. 1012-2004
- NUREG/CR-6101, Sections 3.1.4, and 4.1.4, "Software Verification and Validation Plan."

The V&V planning processes used for the HFC-FPGA platform are described in Sections 5.4, “FPGA Software Development Process” and 5.5, “FPGA Specific Implementation” of the HFC-

FPGA platform TR, (References 2 & 3). QA management and the provision for V&V oversight are the responsibility of a QA Department at HFC that is separate from the other departments responsible for a project. For each project, a QA manager is identified, and a V&V team is specified. The QA manager is responsible for overseeing QA activities and the V&V team performs independent evaluation of the processes and products for lifecycle implementation.

The Software Lifecycle and V&V programs specify development of a master schedule with V&V activities keyed to lifecycle phases, which are defined to be consistent with the lifecycle processes identified in IEEE Std 1074-2006, “IEEE Standard for Developing a Software Project Life Cycle Process” and IEEE Std 1012-2004, "IEEE Standard for Software Verification and Validation." Tasks for V&V at each lifecycle phase are identified for each type of project and the corresponding lifecycle inputs and outputs are specified.

Methods and tools for conducting V&V activities are identified as part of the V&V process. Software development tools are identified in development plans for specific projects. The development tools are maintained under configuration control and the software products generated by their use are subjected to the full range of V&V activities, such as inspections and tests, that are prescribed by the software lifecycle procedure and the associated V&V work instructions.

This V&V process description identifies V&V activities that are conducted for each phase of the development lifecycle. See Section 3.3.1.2 of this SE for a description of the integrity scheme used for the HFC-FPGA platform.

The HFC-FPGA development organization includes several functional teams including; a Research and Development team, a Quality Assurance (QA) team, and a V&V team. The degree of independence established between each of these teams, based on project requirements, is provided by project work instructions that define organizational roles and responsibilities. Aspects of independence between these teams include management, budget and schedule. The QA team and the V&V team are independent from the development teams. FPGA programming is treated as SIL level 4 as defined in IEEE Std. 1012-2004. The NRC staff finds that the HFC approach to independence of V&V for the HFC-FPGA platform complies with the guidance of IEEE Std. 1012-2004 as endorsed by RG 1.168 and is, therefore, acceptable.

The basis for V&V planning is contained in HFC processes, procedures, and plans. These documents provide for development of a program that includes specified V&V tasks integrated into the lifecycle phases for a platform development project. The specification of organizational responsibilities, determination of methods, identification of V&V tasks with defined inputs and outputs, and establishment of documentation conventions provide measures to ensure that development and maintenance activities for the HFC-FPGA platform are performed at an acceptable level. The existing organization structure and specified assignment of V&V roles provide acceptable independence of the V&V team from the project development team and its design activities. Based on this review, the NRC staff has determined that the procedures for establishing a V&V plan exhibit the management, implementation, and resource characteristics identified in SRP BTP 7-14 and are, therefore acceptable.

No evaluation of HFC-FPGA application logic development V&V processes could be performed because no plant specific application was available during this evaluation. See PSAI 5.2.2 for more information on V&V activity oversight to be performed during application development.

3.3.1.7 Configuration Management Planning

Criteria used to evaluate HFC-FPGA Configuration Management (CM) planning was derived from the following:

- RG 1.169
- RG 1.173
- SRP BTP 7-14, Section B.3.1.11, “Software Configuration Management Plan (SCMP),”
- SRP BTP 7-14, Section B.3.2.3, “Acceptance Criteria for Software Configuration Management Activities.”
- IEEE Std. 1074-2006, Clause A.1.2.2, “Plan Configuration Management,”
- IEEE Std. 828-2005, “IEEE Standard for Configuration Management Plans,”
- IEEE Std. 7-4.3.2-2003, Clause 5.3.5, “Software configuration management,”
- IEEE Std. 7-4.3.2-2003, Clause 5.4.2.1.3, “Establish configuration management controls.”
- NUREG/CR-6101, Sections 3.1.3, and 4.1.3, “Software Configuration Management Plan.”

The HFC CM processes are described in Section 5.8 of the HFC-FPGA platform TR, “HFC Configuration Management” (References 2 & 3). The CM processes are applicable to all HFC control system products and projects. This includes the HFC-6000 platform which was previously evaluated by the NRC (Reference 5). The CM processes also apply throughout the safety lifecycle of platform and project specific applications. The HFC-FPGA platform TR describes methods for identifying platform logic element configuration items that are controlled in accordance with the configuration management program. The CM process also defines methods used to establish and maintain configuration control when changes to module FPGA logic are made as well as methods for recording and reporting the status of design changes.

A management review team, composed of a department director or designee, a QA manager, and a V&V manager, is used for approving and managing the implementation of changes to the HFC-FPGA platform. This management review team also provides oversight and direction for the CM processes. The HFC CM plan establishes criteria for establishment of the management review team and describes the configuration control processes including those used for system logic development. These processes include change initiation, change control and change approval.

During a regulatory audit, the NRC staff reviewed HFCs use of configuration management tools to control access to documents and system logic implementation files, manage system change requests, and track changes. The NRC staff also reviewed configuration management procedures as well as configuration management forms. The NRC staff’s observations during the audit support a finding of reasonable assurance that appropriate configuration management activities are being performed. The results of this audit are documented in Reference 13.
The NRC staff concludes that CM planning processes used to support HFC-FPGA platform development are consistent with the criteria of IEEE Std. 828-2005, as endorsed by RG 1.169. This meets the criteria of BTP 7-14 Clause 3.4.1.7 and is, therefore, acceptable.

3.3.1.8 Test Planning and Implementation

Criteria used to evaluate HFC-FPGA test planning and implementation were derived from the following:

- RG 1.170
- RG 1.171
- SRP BTP 7-14, Sections B.3.1.12, “Software Test Plan (STP)” and B.3.1.12
- IEEE Std. 829-2008, “Test Documentation”
- IEEE Std. 1008-1987, “Software Unit Testing.”

Testing for HFC products and projects are governed by quality process procedures for design control and the product lifecycle and V&V program. Procedures for performing test planning activities define organizational roles and responsibilities. The V&V team is responsible for the generation and evaluation of test plans while the design engineers are responsible for generation of test procedures and the execution of tests.

The HFC test planning scope includes qualification, acceptance and integration test activities to be performed during the various phases of the product lifecycle. These tests include individual component testing, prototype testing of modules, qualification testing of applications, and acceptance testing of systems. When system modifications are performed, an analysis is performed to determine the degree of regression testing to be performed. This includes validation of modified FPGA logic.
Preparation of test plans, procedures and reports may be performed either by the V&V team or the project development team. In the later case, the V&V team oversees the conduct of these validation activities by reviewing documentation and witnessing tests. The V&V team also confirms that the test procedures for system validation are developed in accordance with the safety plan, address the requirements of the design, and encompass the full range of usage for the system. Documentation produced in the execution of the QA program includes test plans, cases, procedures and reports. Traceability of all tests performed on software elements is maintained under configuration management control.

The elements of a software test plan to support development and maintenance of the HFC-FPGA platform are provided by the procedures for establishing software lifecycle plans, for performing V&V activities and for controlling designs. The NRC staff determined that HFC processes and procedures for establishing a test plan exhibit the management, implementation, and resource characteristics identified in SRP BTP 7-14 and are, therefore, acceptable. Application logic test plans were not included in the HFC-FPGA platform TR submittal and were therefore not within the scope of the NRC staff’s SE. Application Test planning oversight is therefore a plant specific action item and should be addressed by PSAI 5.2.2.

3.3.2 Logic Implementation and Design Output Documentation

This section summarizes the evaluation of implementation and design output documentation for the HFC-FPGA platform logic. This documentation corresponds with the safety lifecycle process implementation information described in SRP BTP 7-14 Section B.2.2, "Software Life Cycle Process Implementation," and Section B.3.2, "Acceptance Criteria for Implementation.” Since the HFC-FPGA platform TR does not identify a plant specific application, many of the documents identified in SRP BTP 7-14 are not relevant for generic review of the platform. For example, operations, maintenance, and training manuals primarily relate to a specific plant

system and support the licensee as the user of that system. Thus, review of these documents was not within the scope of this evaluation. See PSAI 5.2.2.

The process for development of HFC-FPGA platform software (firmware) and FPGA application logic is described in Section 5.4, “FPGA Software Development Process” of the TR. The following sections describe and evaluate the logic implementation and design documentation associated with the FPGA logic development processes.

3.3.2.1 Safety Analysis

Criteria used to evaluate HFC-FPGA safety analysis activities was derived from the following:

- SRP, BTP 7-14, Section B.3.2.1, "Acceptance Criteria for Safety Analysis Activities"
- NUREG/CR-6101 and RG 1.173, Section C.3, "Software Safety Analyses"

Documentation of HFC-FPGA Safety Analysis implementation is provided by the following:

- HFC TR Section 6.9.3, “Compliance with IEEE Standards”
- PP004-000-01, “Software Safety Plan”
- HFC V&V Phase Reports

HFC performs a safety analysis activity during the requirements, design, implementation and test phases of product development. These analyses are V&V activities and the results of these analyses are reported in the associated phase reports.

The NRC staff reviewed the HFC Software Safety Plans during a regulatory audit and determined that HFC-FPGA platform safety requirements are adequately addressed. The software safety plan shows that identification of potential system hazards is performed during each phase of the development lifecycle. Requirements, design elements, and logic elements that could affect safety are identified and safety impacts are addressed during software development. The results of this audit are documented in Reference 13.

The NRC staff determined that HFC-FPGA platform safety analysis planning activities are acceptable and are compliant with SRP BTP 7-14, Section B.3.2.1. Application level safety analysis task reports were not included in the HFC TR submittal and were therefore not within the scope of the NRC staff’s SE. Oversight of application safety analysis activities are therefore a plant specific action item and should be addressed by PSAI 5.2.2.

3.3.2.2 V&V Analysis and Reports

Criteria used to evaluate HFC-FPGA V&V analysis activities was derived from the following:

- IEEE 7-4.3.2-2003, Clause 5.3.3, “Verification and Validation,” and Clause 5.3.4, “Independent Verification and Validation (IV&V) requirements”
- SRP, BTP 7-14, Section B.3.2.2, "Acceptance Criteria for Software Verification and Validation Activities"

The HFC V&V Plan identifies reports to be produced to document the results of V&V activities performed. The NRC staff reviewed the following documents to support this evaluation:

- WI-VV-004, Requirement Traceability Matrix and Traceability Analysis
- Failure Modes and Effects Analysis (FMEA) Report (Reference 10)
- Test Reports, see audit report (Reference 13) for list of test reports reviewed

HFC-FPGA development V&V activities are documented by a V&V plan which is produced at the initiation of a project, and a final V&V report that is produced at the end of a project. The V&V Plan for the HFC-FPGA system follows HFC work instruction WI-VV-201, "Project Verification and Validation Procedures." See Section 3.3.1.6 of this SE for the NRC evaluation of the HFC V&V Planning processes.

The NRC staff verified that management, implementation and resource V&V planning procedures were established to support V&V activities of the HFC-FPGA platform. The NRC staff reviewed several V&V reports during the regulatory audit to evaluate the degree to which planned V&V activities were accomplished during platform development. The results of this audit are documented in Reference 13. The NRC staff determined the HFC V&V test reports adequately describe a detailed and thorough V&V effort. The overall V&V plan was implemented in a manner, which supports the development of platform logic that will perform required safety functions. The NRC staff found that activities performed and documented in the V&V reports provide reasonable assurance that V&V efforts were effectively implemented to support the development of a product that is suitable for use in safety-related nuclear applications. The V&V reports are written such that the information reviewed, level of detail, and findings of the V&V effort are understandable and informative. The V&V Reports provide adequate documentation to show that V&V tasks were successfully accomplished for each safety lifecycle phase.

Problems and test failures identified during the V&V effort were provided to the HFC corrective action program. Several test and anomaly reports were reviewed during the regulatory audit. The NRC staff found that problem descriptions and actions required to correct or mitigate each problem were adequately documented. Corrective action documentation was also reviewed and was found to be effectively addressing issues and adverse conditions identified during product V&V test activities.

The NRC staff concludes that the development functional and process characteristics of the HFC V&V effort are acceptable. V&V activities performed for the HFC-FPGA platform logic development are acceptable and are compliant with SRP BTP 7-14, Section B.3.2.2. See PSAI 5.2.2 for oversight activities to be performed during application logic development.

3.3.2.3 Requirements Traceability Evaluation

Criteria used to evaluate the HFC requirements traceability processes were derived from the following:

- SRP, BTP 7-14, Sections A.3 and B.3.3, "Acceptance Criteria for Design Outputs"
- SRP, BTP 7-14, Section B.3.2.2, "Acceptance Criteria for Software Verification and Validation Activities"
- SRP, BTP 7-14, Section B.3.2.3, "Acceptance Criteria for Software Configuration Management Activities"

The HFC-FPGA TR describes traceability analysis as; *"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."* The TR also states; *"All changes to requirement specifications are evaluated to determine any impact on other phases in the design process as part of the Configuration Management Analysis and Requirements Traceability Analysis of each phase."*

Traceability of HFC-FPGA platform requirements and derivative requirements between documents is established by a requirement traceability matrix (RTM). Establishment and verification of requirements traceability are defined as V&V activities that are performed at various stages of the HFC-FPGA development lifecycle. A requirement tracing tool is used to implement traceability. This tool is used to support audits and analysis activities to access status and completion of requirements.

The NRC staff observed the use of the HFC-FPGA traceability tool and reviewed several selected requirement threads during the regulatory audit. The NRC staff was able to trace selected requirements to implementation and test documents and verify that traceability was established and maintained. The results of this audit are documented in Reference 13.

The NRC staff observed that the HFC-FPGA platform RTM shows each of the requirements delineated in requirements specifications are broken down into sub-requirements. The RTM identifies implementation documents and test requirements credited to address each system requirement. The RTM refers to documented evidence to show that each system requirement has been implemented in the platform hardware and logic design and shows that V&V testing has been performed to demonstrate correct implementation of each requirement.

The NRC staff determined that requirements tracing processes used for the HFC-FPGA platform hardware and logic implementation provide reasonable assurance that all requirements are correctly implemented and are consistent with BTP 7-14 criterion and are therefore acceptable.

The HFC-FPGA platform TR does not address traceability activities associated with plant application specific logic. Therefore, plant application requirements traceability activities for HFC-FPGA platform-based safety systems must be performed during plant application development and thus were not evaluated in this SE. See PSAI 5.2.2 for additional information on providing oversite for application development activities.

3.3.2.4 Configuration Management Activity

The criteria were used to evaluate the HFC configuration management activities were derived from the following:

- IEEE 7-4.3.2-2003, Section 5.3.5, “Configuration Management”
- IEEE Std. 828-2005, “IEEE Standard for Configuration Management Plans”
- BTP 7-14, Section B.3.2.3, “Acceptance Criteria for Software Configuration Management Activities”

The HFC CM plan establishes requirements for implementation of a CM process during the safety lifecycle of HFC-FPGA systems. This CM plan describes CM tasks that are performed by HFC. See Section 3.3.1.7 of this SE for the NRC evaluation of the HFC CM planning processes.

CM activities are performed in accordance with work instruction WI-ENG-003, “Configuration Management”. This work instruction was previously evaluated for the HFC 6000 microprocessor-based platform and was found to be acceptable. During the regulatory audit, the NRC staff reviewed several CM documents and confirmed that the activities outlined in the CM plan were being performed.

Configuration Item status accounting for the HFC-FPGA platform consists of the recording and reporting of the information that is needed to manage project components effectively, including a listing of the approved component identification, the status of proposed changes to the components, and the implementation status of approved changes.

The HFC audit process is used to ensure that records are being generated and maintained. Configuration audit reports provide documentation of configuration management activities performed during each phase of platform component development. Configuration audits of the HFC Software Configuration Management process and records are performed at the end of each lifecycle phase. These audits provide a check of correctness of the HFC configuration item functional and physical features.

HFC maintains and controls platform design documentation and program files as QA records. Changes to controlled files are tracked and can only be changed by using a system change requests (SCR) process. The HFC SCR process is implemented by work instruction WI-ENG-812 "System Change Request (SCR) Procedures" which was also evaluated during the HFC 6000 platform SE and was found to be acceptable. During a regulatory audit, the NRC staff reviewed the HFC work instructions for performing system design changes and conducted an exercise involving making a sample logic change using these procedures. The results of this audit are documented in Reference 133.

During the regulatory audit, The NRC staff reviewed the HFC-FPGA master document list as well as several condition reports and software change requests to gain an understanding of how HFC-FPGA platform configurations were being captured and controlled in accordance with the HFC configuration management program described in Section 5.8 of the HFC-FPGA platform TR, "HFC Configuration Management". The CM documentation reviewed was found to contain an adequate level of information to show that the configuration management plan is being carried out in its entirety and that changes made to items under configuration control are being controlled, tracked, and documented in a manner which is consistent with a high-quality development process.

The NRC staff determined the CM processes which include activities performed to establish and maintain configuration control meet the requirements of IEEE Std. 828-2005 and ANSI/IEEE Standard 1042-1987 and are therefore acceptable. The HFC CM activities adequately address the guidance in BTP 7-14 Section B.3.2.3.

3.3.2.5 Failure Modes and Effects Analysis

The following criteria were used for evaluating the HFC-FPGA platform FMEA:

- GDC 23, "Protection System Failure Modes"
- RG 1.53
- IEEE Std. 379-2000, Clause 5.5, "Single Failure Criteria / Common Cause Failures"

The NRC staff reviewed the HFC-FPGA platform FMEA methodology described in Section 6.7 of the HFC-FPGA platform TR (References 2 & 3) and RR901-107-11, "FMEA for the HFC-FPGA Platform Functions and System" (Reference 10).

The FMEA was performed to address the failure modes of all major active components of the HFC-FPGA platform. The HFC FMEA scope included all platform modules and communications interfaces. The FMEA analyzes potential failures in each of the component

groups and describes the symptomatic and system level effects of these failures. The FMEA also identifies the method of detection for each postulated failure mode.

The NRC staff notes that several of the postulated failure modes analyzed in the FMEA did not identify a method for detection however, the effects of these failures did not have any impact on the system safety functions. Instead, the failures resulted in a reduction of system in-channel redundancy. Because a safety system based on the HFC-FPGA platform would include multiple safety division redundancies, the impact of these failures does not compromise a system's ability to meet the single failure criteria in IEEE Std. 603-1991, Section 5.1.

The results of this FMEA show that major potential hardware failures have a known and deterministic method of failure, each of which is detectable by the HFC-FPGA system and can therefore be communicated to the user. The HFC FMEA results also indicated that several of the platform modules rely upon application software functions or manual surveillance tests for detection of failures.

Because the failure analysis was performed at platform level, the FMEA did not demonstrate that input signal or system level failures would cause an HFC-FPGA platform-based safety system to revert to a predefined safe state for all cases. The fail-safe states for HFC-FPGA safety functions are also not generically defined and must be determined as a specific application development activity. Therefore, a system level FMEA should be performed during plant specific application development to identify potential system level failure modes and to determine the effects of these failure modes on plant safety. PSAI 5.2.9 of this SE identifies additional actions which must be addressed during specific plant application development.

3.3.2.6 Reliability Analysis

The following criteria were used to evaluate HFC-FPGA platform reliability characteristics.

- RG 1.152
- IEEE Std. 352-1987, "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems"
- IEEE Std. 603-1991, Clause 5.15, "Reliability"
- IEEE Std. 603-1991 Clauses 6.7 and 7.5, "Maintenance Bypass."

A reliability analysis for the HFC-FPGA modules was performed using guidance from IEEE Std 352-1987, and the mathematical models developed in military handbook, MIL-HDBK-217F, "Reliability Prediction of Electronic Equipment."

Section 6.9.3 of the HFC-FPGA platform TR includes a description and summary of the reliability analysis performed for the platform. This description includes a table which lists failure rates and availability values associated with HFC-FPGA modules. This reliability data can be used to support a system-level reliability and availability analysis. Because reliability goals are established on a plant specific basis, a determination of whether plant and system specific goals are met must be made at the time of application development. PSAI 5.2.10 of this SE identifies additional reliability analysis activities, which must be performed during plant specific application development.

3.3.2.7 Design Specification Review

The following criteria were used to evaluate HFC-FPGA platform design specifications.

- NUREG-0800, BTP 7-14, Section B.3.3.1, “Requirements Activities - Software Requirements Specification”
- RG 1.172
- IEEE Std. 830-1998, "IEEE Recommended Practice for Software Requirements Specifications”
- NUREG/CR-6101, Sections 3.2.1 and 4.2.1 “Life Cycle Software Reliability” and “Safety Activities”

The NRC staff’s review in this area focused on clarity and completeness of HFC-FPGA platform requirements and relied on thread audits to confirm that requirements were traceable through applicable platform design documentation. Section 3.3.2.3 of this SE describes these requirement thread reviews.

The NRC staff reviewed HFC-FPGA platform contract / system requirement documentation, requirement specifications, design specifications, and test specifications during regulatory audit (Reference 13). During the audit, the RTM was used to verify requirement traces performed by the NRC staff. The audit showed that HFC-FPGA design documents accurately reflect the platform requirements and exhibited the functional and platform logic development process characteristics necessary to facilitate the development of quality programmable logic for use in nuclear safety applications. The NRC staff determined that the requirements documentation is adequately controlled by vendor processes, which include the use of a verification checklist and a process for providing feedback to the design team.

3.4 Equipment Qualification

The purpose of performing EQ testing for a safety system are (1) to demonstrate that the safety system will not experience failures due to both normal and abnormal service conditions of temperature, humidity, radiation, electromagnetic interference (EMI), radio frequency interference (RFI), electrical fast transient (EFT), electrostatic discharge (ESD), electrical power surge, or seismic; and (2) to verify those tests meet the plant-specific requirements.

Criteria of EQ for safety-related equipment are provided in 10 CFR Part 50, Appendix A, GDC 2, and GDC 4. Additionally, the regulation 10 CFR 50.55a(h) incorporates by reference the requirements of IEEE Std. 603-1991 which addresses both system-level design issues and EQ criteria for qualifying devices. RG 1.209, endorses and provides guidance for compliance with IEEE Std. 323-2003, “IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations” for qualification of safety-related computer-based I&C systems installed in mild environment locations. RG 1.180, endorses and includes guidance for conformance with MIL-STD-461E, “Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment” and IEC 61000 series standards for evaluation of the impact of EMI, RFI, EFT, and electrical power surges on safety-related I&C systems. RG 1.100, provides an endorsement of IEEE Std. 344-2004, “IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations” with exceptions and clarifications, and describes methods that the NRC staff considers acceptable for use in seismic stress qualification of electrical and active mechanical equipment.

To comply with the requirements of GDC 4 and IEEE Std. 603-1991, an applicant must demonstrate through EQ that safety-related I&C systems meet design-basis and performance requirements when the system equipment is exposed to normal and adverse environments. But, the HFC-FPGA platform equipment is evaluated in this SE for use in mild environmental conditions only, as defined in 10 CFR 50.49(c) and therefore, the requirements for equipment in harsh environments of 10 CFR 50.49 are not applicable (see PSAI 5.2.6). In addition, the EQ for the HFC-FPGA platform evaluated in this SE does not include the smoke stress test. Although smoke has the potential to be a significant environmental stressor that can result in adverse consequences on digital I&C systems, the most effective approach for addressing smoke susceptibility is to minimize the likelihood of smoke exposure by rigorously adhering to the fire protection requirements in 10 CFR Part 50.48, “Fire Protection,” or other individual plant license commitments (see PSAI 5.2.7).

Section 5.4.2 of SRP Chapter 7, Appendix 7.1-D, “Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2-2003” states that EPRI TR-107330, “Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-related Applications in Nuclear Power Plants” provides specific guidance for the evaluation of commercial grade digital equipment and existing programmable logic controllers (PLCs). The relevant guidance in EPRI TR-107330 is applicable to assess the EQ of FPGA-based control platforms although FPGA-based platforms are not specifically labeled as a PLC. EPRI TR-107330 presents a specification in the form of a set of requirements to be applied to the generic qualification of PLCs for application and modification to safety-related I&C systems in NPP. It is intended to provide a qualification envelope corresponding to a mild environment that should meet regulatory acceptance criteria for a wide range of plant-specific safety-related applications.

The qualification envelope that is established by compliance with the guidance of EPRI TR-107330 consists of the maximum environmental and service conditions for which qualification was validated and the range of performance characteristics for the PLC platform that were demonstrated under exposure to applicable stress conditions. Any licensee who plans to use the HFC-FPGA platform is obligated to verify that the requirements of its specific application are bounded by the established qualification envelopes in the approved Amendment for HFC-FPGA System of HFC-6000 safety platform TR (References 2 & 3) and its associated HFC-FPGA Equipment Qualification Summary Test Report (Reference 9). See PSAI 5.2.5 if the application specific environmental and other conditions are not covered by the condition envelopes used to qualify the HFC-FPGA platform.

HFC used the guidance provided in EPRI TR-107330 to establish the testing approach to meet the criteria of IEEE Std. 323-2003 as endorsed by RG 1.209 for environmental stress qualification, IEEE Std. 344-2004 as endorsed in RG 1.100 for seismic stress qualification, and MIL-STD-461E and IEC 61000 series standards as endorsed in RG 1.180 for electromagnetic compatibility (EMC) qualification. The qualification program developed for the HFC-FPGA platform addressed EQ for a mild, controlled environment, such as the main control room and auxiliary I&C equipment rooms.

EQ testing of environmental stresses for the HFC-FPGA platform was performed by a company named Environmental Testing Laboratory (ETL), Inc. located in Dallas, Texas in accordance with criteria in RG 1.209, its endorsed IEEE Std. 323-2003, and relevant guidance in EPRI TR-107330 to demonstrate performance under a variety of environmental conditions. ETL also provided seismic stress qualification testing services according to criteria in RG 1.100, its endorsed IEEE Std. 344-2004, and applicable guidance in EPRI TR-107330. HFC contracted with National Technical Systems (NTS) located in Plano, Texas to perform EMC qualification

testing, which includes EMI/RFI emissions and susceptibility, EFT, ESD, and electrical surge withstand capacity (SWC) in accordance with criteria in RG 1.180 and its endorsed MIL-STD-461E and IEC 61000 series standards. Laboratory testing services were performed in accordance with the HFC services procurement specification. Radiation qualification testing was not performed for the HFC-FPGA platform because the HFC-FPGA platform equipment assessed in this SE is expected to be installed in mild environments only (see PSAI 5.2.6).

A description of EQ for the HFC-FPGA platform was provided in Section 8 of the HFC-FPGA platform TR. In addition, test plans, procedures, and results were submitted to the NRC for review. For the HFC-FPGA platform EQ, a qualification test specimen (QTS) was developed and then used during all EQ test activities. This QTS was developed in accordance with EPRI TR-107330 and includes a representative sampling of the HFC-FPGA platform modules which are listed in the following table for evaluation and qualification testing.

Table 3.4-1 Qualified Modules in Qualification Test Specimen

Designation	Part Number	Function	Bill-of-Material (BOM) Part Number	BOM Revision
HFC-FPUD01	40117421Q	16-Point Form C Relay Output Card	40117481	C
HFC-FPUD02	40117422Q	FPU I/O Module for 32 DI Channels	40117442	B
HFC-FPUA01	40124221Q	FPU I/O Module for 16 4- to 20-mA AI Channels	40124241	B
HFC-FPUAO	40129421Q	FPU I/O Module for 8 4-to 20-mA AO Channels	40129481	F
HFC-FPUL	40127021Q	FPU I/O Module for 8 AI Channels for Type E Thermocouples	40127081	C
HFC-FPUM	40127421Q	FPU I/O Module for 8 AI Channels for 100-OhmPlatinum RTDs	40127441	A
HFC-FPUM2	40145621Q	FPU I/O Module for 8 AI Channels for 100-OhmPlatinum RTDs (designed for a higher input accuracy)	40145641	A
HFC-FCPU	40132221Q	FPGA Controller Module for the HFC-FPGA system with onboard I/O function	40132241	A
HFC-FCPUX	40145221Q	FPGA Controller Module for the HFC-FPGA system	40145241	A
HFC-HSIM	40108621Q	F-Link High Speed Interface Module	40108681	D

HFC-FPC08	40103834Q	Communication Gateway Controller Without VGA	40103896	A

The QTS also includes supporting equipment which is used to interface with the HFC-FPGA modules in a manner comparable to how they would be implemented in a typical plant application setting, but the supporting equipment is excluded from qualification as stated in the HFC-FPGA platform TR. Only the specific HFC-FPGA platform modules listed in the Table 3.4-1 are qualified. HFC-FPGA auxiliary components are listed in Table 3.2-2 of this SE. For specific applications referencing the HFC-FPGA platform, different HFC-FPGA platform modules or same modules with different versions need to be qualified (see PSAI 5.2.8).

A test specific application program (TSAP) used for the HFC-FPGA QTS was also developed by following guidance in EPRI TR-107330 to demonstrate capabilities comparable to those that would be required in a plant-specific application. The TSAP was specifically designed and implemented in the QTS to support qualification testing of the HFC-FPGA platform modules while providing generic functionality of the test system.

The qualification process consisting of pre-qualification, qualification, and post-qualification tests was planned and performed on the QTS according to guidance in EPRI TR-107330, including a defined set of operability and prudency tests which were conducted for pre-qualification, after each of qualification tests (including environmental stress testing, EMI/RFI testing, ESD/EFT/SWC testing, and seismic testing), and post-qualification. The testing results were retained, analyzed for compliance with the acceptance criteria, and documented. Baseline testing was periodically performed during the complete qualification process to monitor for impacts on performance of the QTS. The QTS was monitored during the qualification tests and any fault messages from the operational diagnostic were noted and evaluated. All self-diagnostics (including hardware watchdog timers) were in operation during qualification tests.

Besides the HFC-FPGA safety platform TR and its Equipment Qualification Summary Test Report, the NRC staff also reviewed the HFC-FPGA EQ testing plans and procedures. The NRC staff finds that the EQ testing program for the HFC-FPGA platform established its qualification envelopes according to the above regulatory guidance. The NRC staff also finds that the basis for the HFC-FPGA EQ testing program was conformance with the guidance contained in EPRI TR-107330. Therefore, the NRC staff considers that the HFC-FPGA EQ testing program acceptable.

3.4.1 Environmental Stress Qualification

The environmental stress qualification test was conducted to show that the physical modules in the HFC-FPGA QTS work within acceptable specifications during heating and cooling. The test was also performed to demonstrate that the HFC-FPGA QTS would not experience failures due to abnormal service conditions of temperature and humidity.

Section 8.2.4.1, “Environmental Stress Qualification Tests” of the HFC-FPGA Platform Topical Report and Appendix B of HFC-FPGA EQ Summary Test Report specify the qualification testing envelope for temperature and humidity. Section 4.3.6.2 of EPRI TR-107330 requires that the generic PLC meet its performance requirements over normal and abnormal environmental conditions. HFC specified temperature and humidity environmental test levels that exceeded these conditions in EPRI TR-107330 with a 5% margin added. Specifically, the environmental stress qualification test included three major phases for qualifying the HFC-FPGA platform

modules: (1) a minimum 48-hour period with the ambient temperature at 145°F at 95% relative humility (RH) and a transition period of 4 hours during which the ambient temperature is reduced to 35°F at 0% RH (non-condensing); (2) a minimum 8-hour period with the ambient temperature at 35°F with 0% (noncondensing); and (3) a transition period of 4 hours during which the test chamber is brought back to ambient room temperature and humidity. The NRC staff finds that the above testing profile met criteria in EPRI TR-107330 for the generic environmental stress qualification.

Environmental stress qualification testing of the HFC-FPGA platform QTS was performed in accordance with EPRI TR-107330 as stated in the HFC-FPGA Platform Topical Report and its Qualification Summary Test Report. The NRC staff evaluated the HFC-FPGA environmental stress qualification test results to determine compliance with the criteria in RG 1.209 and IEEE Std. 323-2003 for mild environment installations and to determine if the EQ test plan was followed. The HFC-FPGA platform QTS performance requirements were verified during and following exposure to abnormal environmental conditions according to a time varying profile that was very similar to the profile shown in Figure 4-4 of EPRI TR-107330. Verification of QTS performance requirements included performance of both operability and prudency tests as defined in the HFC-FPGA EQ test plans and test procedures. The NRC staff confirmed that EPRI TR-107330, Sections 4.3.6, “Environmental Requirements” and 6.3.3, “Environmental Testing Requirements” criteria were met.

The HFC-FPGA test configuration was designed to produce the worst-case temperature rise expected across the HFC-FPGA module chassis as is specified in Section 6.2.1.1 of EPRI TR-107330. The HFC-FPGA platform QTS was monitored before, during and after each test to confirm that no equipment failures or abnormal functions occurred. System self-diagnostics were also functioning as an integral feature of the HFC-FPGA QTS design. During the test, two alarms occurred briefly but were cleared automatically. Another alarm for the redundancy interface was detected but found to be caused by a damaged cable. This issue was resolved by replacing the damaged cable. In general, no system abnormalities were detected during tests.

To demonstrate PLC performance in specified environmental conditions, Section 4.3.6.3 of EPRI TR-107330 requires that the test PLC operate for the environmental (temperature and humidity) stress test profile given in Figure 4-4 of this EPRI technical report. Environmental testing profiles used for HFC-FPGA QTS are provided in both Figure 24 of the HFC-FPGA Platform Topical Report and in Figure 6 of Appendix B of the HFC-FPGA Equipment Qualification Summary Test Report.

The NRC staff finds that the environmental profile for the HFC-FPGA platform QTS is compliant with the methodology outlined in Section 4.3.6.3 of EPRI TR-107330. The NRC staff reviewed the test results included in the HFC-FPGA Qualification Summary Test Report and verified against corresponding results in its detailed test report TR901-302-01, “HFC-FPGA Control System of HFC-6000 safety platform qualification test report” (Reference 15). The NRC staff also found that a pre-qualification acceptance test was performed prior to subjecting the HFC-FPGA QTS to the environmental conditions profile and a series of operability checks was performed at various environmental conditions during profile execution. The NRC staff determined that the HFC-FPGA QTS operated satisfactorily during these tests and all operability and prudency tests were also completed satisfactorily.

Therefore, the NRC staff finds that the HFC-FPGA platform modules in the above Table 3.4-1 is therefore acceptable for installations where environmental conditions do not exceed the environmental condition profile established for the HFC-FPGA platform qualification in this SE.

See PSAI 5.2.5 for applications with environmental conditions unbounded by the profile evaluated in this SE.

3.4.2 Class 1E to Non-1E Isolation Qualification

In Section 6.3.6, "Class 1E / Non-1E Isolation Requirements," of EPRI TR-107330, it states, in part, that Class 1E to non-1E isolation capability testing shall be performed per the requirements of Section 4.6.4, "Class 1E/Non-1E Isolation Requirements". However, during the audit on the HFC-FPGA platform in May 2020 (Reference 13), the NRC staff found that the Class 1E to Non-1E isolation capability testing had not been conducted as part of the EQ to qualify the HFC-FPGA platform. So, HFC created the Condition Report No. 2020-0093 to document this non-conformance, analyzed its root causes, and specified a corrective action plan to perform this isolation capability testing (Reference 16).

IEEE Std. 384, "Standard Criteria for Independence of Class 1E Equipment and Circuits", states, in part, that: (1) the isolation device prevents shorts, grounds, and open circuits on the Non-Class 1E side from unacceptably degrading the operation of the circuits on the Class 1E side, and (2) the isolation device prevents application of the maximum credible voltage on the Non-Class 1E side from degrading unacceptably the operation of the circuits on the Class 1E side. Section 6.3.6 of EPRI TR-107330 also states, in part, that for I/O modules the surge only needs to be applied to a representative sample of the points for a given module type.

In September 2020, HFC conducted the isolation capability testing for the HFC-FPGA platform in accordance with IEEE Std. 384 and Section 6.3.6 of EPRI TR-107330. The isolation capability testing for the HFC-FPGA platform was performed at the HFC test facility as part of the EQ test program to demonstrate its compliance with applicable Class 1E to Non-1E isolation capability requirements and acceptance criteria in EPRI TR-107330 and IEEE Std. 384. The isolation capability testing details and results are provided in the "HFC-6000 Control System VV0115 Isolation Test Summary Report" (Reference 17).

The NRC staff reviewed the above isolation test summary report and found that the same HFC-FPGA QTS as listed in Table 3.4-1 of this SER and utilized for other EQ tests was used for this isolation capability testing. This isolation test summary report has documented the results of executing the HFC Isolation Test Procedure, TP901-200-07, Rev. E for the HFC-FPGA Control System (Reference 17). The testing summary is created from the results of the executed corrective action test plan that addressed the test approach, equipment to be tested, sequence of testing, test procedures, test specimen mounting, test conditions, test levels, performance monitoring, acceptance criteria, and documentation.

For the Class 1E to Non-1E isolation qualification, the HFC-FPGA platform intended for nuclear safety-related applications is based on a system design that permits Non-Class 1E connections to the analog and discrete input and output interfaces. The testing sequence for the HFC-FPGA platform included the following isolation capability tests performed on the QTS modules:

- 4 to 20 mA analog inputs for HFC-FPUA module,
- RTD inputs for HFC-FPUM2 and HFC-FPUM module,
- TC inputs for HFC-FPUL module,
- 48-VDC discrete inputs for HFC-FPUD02,
- 4 to 20 mA analog outputs for HFC-FPUAO module, and
- Relay discrete outputs for HFC-FPUD01 module.

The isolation capability tests were performed to demonstrate electrical isolation of Class 1E control equipment from Non-Class 1E equipment as well as isolation between different Class 1E channels. The isolation capability tests for the HFC-FPGA modules were performed by applying both 600 VAC and 250 VDC for 30 seconds with automated operability and prudency tests conducted to verify that no module(s) other than the one under test is affected. During the tests, specific static points on each module under test were monitored to detect any deviation caused by the applied test signals. The operation of the HFC-FPGA QTS was monitored, and system performance data was recorded. The NRC staff finds that how the isolation capability tests were run on the HFC-FPGA QTS meets the Class 1E and Non-1E isolation testing criteria in EPRI TR-107330.

The NRC staff reviewed the testing results which can be summarized below: For 4 to 20 mA analog inputs on the HFC-FPUA module, after applying the 600 VAC and 250 VDC for 30 seconds, no module other than the HFC-FPUA module being subjected to the test signals was affected on the HFC-FPGA QTS. For RTD inputs on both the HFC-FPUM2 and HFC-FPUM modules, isolation capability tests were performed by using both the 600 VAC and 250 VDC as test signals for 30 seconds. The test results show that all other modules other than the module under test were not impacted. For TC inputs for the HFC-FPUL module, both test signals 600 VAC and 250 VDC were applied separately for 30 seconds to test its isolation capability. The recorded testing results demonstrate that the isolation capability tests passed without adverse effect on all other modules on the HFC-FPGA QTS during the tests.

For 48-VDC discrete inputs for the HFC-FPUD02 module, test signals 600 VAC and 250 VDC were also applied for 30 seconds to test the isolation capability for this module. During the tests, no impacts were recorded on all other modules on the QTS. For 4 to 20 mA analog outputs for the HFC-FPUAO module, the test results show that no module other than the HFC-FPUAO module subjected to the test signals was affected, and no other channel on the same HFC-FPUAO module under test was changed by more than 0.05% after applying the test signals 600 VAC and 250 VDC for 30 seconds. For relay discrete outputs for the HFC-FPUD01 module, after utilizing both the test signal 600 VAC and 250 VDC as test signals for 30 seconds, no disruption in operation of any other module occurred on the HFC-FPGA QTS.

During the Class 1E to Non-1E isolation capability tests, automated operability and prudency testing of the HFC-FPGA QTS was conducted according to the HFC test procedures, and results of these automated tests showed that no degradation of the HFC-FPGA QTS happened. The NRC staff reviewed the HFC-FPGA isolation qualification test summary report, test procedures, and test results and determined that the HFC-FPGA platform met the acceptance criteria in Sections 4.6.4 and 6.3.6 of EPRI TR-107330 and IEEE Std. 384 for all tested modules on the HFC-FPGA QTS. It is the responsibility of the licensee to verify that maximum test voltages cited in the Isolation Test Summary Report to which the HFC-FPGA platform equipment is qualified to operate are not exceeded for all HFC-FPGA Class 1E to Non-Class 1E interfaces (see PSAI 5.2.18).

3.4.3 Electromagnetic Compatibility (EMC) Qualification

RG 1.180 endorses MIL-STD-461E, “Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment,” and IEC 61000 series standards for evaluating the impact of EMI, RFI, EFT, ESD, and electrical power surge on safety-related I&C systems.

EPRI TR-107330 includes electromagnetic compatibility (EMC) testing as part of the overall program to generically qualify a PLC for safety-related applications in NPPs. Specific criteria for EMI/RFI, ESD withstand, power surge, and isolation capability are given in Sections 4.3, "Hardware Requirements," and 4.6, "Electrical" while the qualification approach is specified in Section 6.3, "Qualification Tests and Analysis Requirements."

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

The EMC testing for qualifying the HFC-FPGA platform modules is described in the HFC-FPGA Platform Topical Report as follows:

- EMI and RFI qualification tests for the HFC-FPGA platform is described in Section 8.2.4.2
- ESD testing is described in Section 8.2.4.3
- EFT and power SWC testing are described in Section 8.2.4.4

EMI, RFI, EFT, SWC, and ESD testing of the HFC-FPGA QTS was performed at the NTS facility located in Plano, Texas. The HFC-FPGA platform QTS was installed in the EMC test chamber in accordance with test specimen mounting criteria in Section 6.3.2.1 of EPRI TR-107330. The HFC-FPGA platform QTS was mounted in a single open chassis. The power to the HFC-FPGA QTS was supplied from a set of 24VDC power supply modules. The power supply modules were not included as part of the HFC-FPGA platform qualification because those power supply modules have the same model and type as those already qualified as part of the previous HFC-6000 platform qualification approved by the NRC. So, the power interruption test of the power supply modules was not conducted for the HFC-FPGA platform QTS.

The HFC-FPGA platform QTS modules were subjected to EMC testing to demonstrate compliance with the applicable criteria for the EMI/RFI, EFT, ESD, and SWC in RG 1.180. The specific test configuration of the HFC-FPGA QTS equipment is described in Section 5.0, "Test System" of the HFC-FPGA Equipment Qualification Summary Test Report. The following subsections describe tests performed and summarize the results obtained.

3.4.3.1 EMI/RFI Emission and Susceptibility Testing

The EMI/RFI testing was performed to show the suitability of the HFC-FPGA platform to be used as a safety-related device with respect to EMI/RFI emission and susceptibility levels. The EMI/RFI testing was also conducted to establish the range and magnitude of EMI/RFI emissions produced by the HFC-FPGA platform QTS and the impact of environmental EMI/RFI noise on the reliable operation of the QTS. The NRC staff found that the EMI/RFI tests on the HFC-FPGA platform QTS as listed below were performed in accordance with criteria in RG 1.180 and guidance in EPRI TR-107330 and TR-102323.

Emission Testing

The following specific EMI/RFI emission tests as required in RG 1.180 were performed on the HFC-FPGA QTS:

- MIL-STD-461E, CE101: “Conducted Emissions, AC and DC Power Leads (30 Hz to 10 KHz)”.
  The frequency range for the CE101 test for the HFC-FPGA QTS is 120 Hz to 10 KHz. The HFC-FPGA QTS is a 120VAC 60Hz driven unit. For alternate current (AC) applications, MIL-STD-461E indicates that for the CE101 test, the frequency should start from the second harmonic of power supply frequency, which is 120 Hertz (Hz) in this case. So, the NRC staff finds that the frequency range (120 Hz to 10 Kilohertz (KHz)) used for the CE101 test is acceptable.
- MIL-STD-461E, CE102: “Conducted Emissions, AC and DC Power Leads (10 KHz to 2 MHz)”
- MIL-STD-461E, RE101: “Radiated Emissions, Magnetic Field (30 Hz to 100 KHz)”
- MIL-STD-461E, RE102: “Radiated Emissions, Electric Field (2 Megahertz (MHz) to 1 Gigahertz (GHz)).”

The frequency range for the RE102 test is from 2 MHz to 18 GHz for the HFC-FPGA QTS. The NRC staff finds that this frequency range is acceptable because range envelopes the required frequency range in MIL-STD-461E for the RE102 test.
The above specific EMI/RFI emission tests and results are provided in Appendix C of the HFC-FPGA Equipment Qualification Summary Test Report.

Susceptibility Testing
The following EMI/RFI susceptibility tests as required in RG 1.180 were conducted for the HFC-FPGA platform QTS:

- MIL-STD-461E, CS101: “Conducted Susceptibility, low frequency (30 Hz to 150 KHz)”. The frequency range for the CS101 test for the HFC-FPGA QTS is 120 Hz to 150 KHz. The HFC-FPGA QTS is a 120VAC 60Hz driven unit. For AC applications, MIL-STD-461E states that for the CS101 test, the frequency should start from the second harmonic of power supply frequency, which is 120 Hz in this case. So, the NRC staff finds that the frequency range (120 Hz to 150 KHz) used for the CS101 test is acceptable.
- MIL-STD-461E, CS114:” Conducted Susceptibility, high frequency (10 KHz to 30 MHz)”
- MIL-STD-461E, CS115: “Conducted susceptibility, bulk cable injection, impulse excitation”
- MIL-STD-461E, CS116: “Conducted susceptibility, damped sinusoidal transients (10 KHz to 100 MHz)”
- MIL-STD-461E, RS101: “Radiated Susceptibility, magnetic field (30 Hz to 100 KHz)”
- MIL-STD-461E, RS103: “Radiated Susceptibility, electric field (30 MHz to 1 GHz).”

The frequency range for the RS103 test for the HFC-FPGA QTS is 30 MHz to 10 GHz. The NRC staff finds that this frequency range is acceptable because the range envelopes the required frequency range in MIL-STD-461E for the RS103 test.

The NRC staff finds that all emission profiles and susceptibility signal levels for the HFC-FPGA QTS were selected to conform to or exceed the requirements of RG 1.180. The test results show that the HFC-FPGA QTS met acceptance criteria during all emission and susceptibility tests. The specific EMI/RFI emissions tests and results are included in Appendix C of the HFC-FPGA Equipment Qualification Summary Test Report.

3.4.3.2 Electrostatic Discharge Withstand Testing

The objective of ESD withstand test is to demonstrate the suitability of the HFC-FPGA platform to be used as a safety-related device with respect to ESD withstand level. Section 4.3.8 of EPRI TR-107330 requires that the HFC-FPGA QTS under qualification be tested for ESD withstand capability in accordance with the requirements of EPRI TR-102323, Revision 1. In accordance with EPRI TR-102323, the specific ESD withstand test to be performed is IEC 61000-4-2 "Electromagnetic Compatibility (EMC), Part 4-2: Testing and Measurement Techniques, Electrostatic Discharge Immunity Test". Specifically, for the HFC-FPGA QTS, contact discharge levels used for the ESD withstand test were 8 kV, applied ten times at a positive polarity and ten times at a negative polarity to each test point. Air discharge levels used for this test were 15 kV, applied ten times at a positive polarity and ten times at a negative polarity to each test point.

The NRC staff found that the ESD withstand testing for the HFC-FPGA platform QTS was conducted in accordance with the HFC-FPGA platform qualification test plan and procedure and conformed to the specific ESD test methods as defined in IEC 61000-4-2. The test results demonstrate that the HFC-FPGA QTS met all acceptance criteria for all points tested. The specific ESD withstand test and results are provided in Appendix D of the HFC-FPGA Equipment Qualification Summary Test Report.

3.4.3.3 Surge Withstand and Electrical Fast Transient Susceptibility Testing

The SWC and electrical fast transient (EFT) susceptibility testing were performed to demonstrate the suitability of the HFC-FPGA platform to be used as a safety-related device with respect to surge withstand levels and EFT. The following tests as required in RG 1.180 were conducted for the HFC-FPGA platform QTS:

- IEC 61000-4-4, "Electromagnetic Compatibility (EMC), Part 4-4: Testing and Measurement Techniques, Electrical Fast Transient/Burst Immunity Test". The EFT used for the HFC-FPGA QTS test is Category B at 4 kV applied to 120 VAC input power and at 500 V coupled into signal lines.
- IEC 61000-4-5, "Electromagnetic Compatibility (EMC), Part 4-5: Testing and Measurement Techniques, Surge Immunity Test". The combination wave used for the test is Category B at 4 kV/2 kV applied to 120 VAC input power.
- IEC 61000-4-12, "Electromagnetic Compatibility (EMC), Part 4-12: Testing and Measurement Techniques, Oscillatory Waves Immunity Test". The ring wave used for the test is Category B at 4 kV applied to 120 VAC input power.

The NRC staff finds that the above SWC and EFT tests were performed on the HFC-FPGA platform QTS in accordance with criteria in RG 1.180 and applicable guidance in EPRI TR-107330. The test results show that the HFC-FPGA QTS met all acceptance criteria during the ring wave, combination wave, and EFT tests. The specific SWC and EFT tests and results are provided in Appendix E of the HFC-FPGA Equipment Qualification Summary Test Report.

3.4.3.4 EMC Testing Results

The EMC test acceptance criteria for the HFC-FPGA platform QTS included monitoring of equipment performance before, during, and after each test. Detailed test acceptance criteria are described in Section 8 of the HFC-FPGA platform TR and in Appendices C to E of the HFC-FPGA Equipment Qualification Summary Test Report. The NRC staff reviewed these

acceptance criteria and found them to be conformance with pertinent guidance in RG 1.180. The NRC staff also confirmed the following major test results:

- The HFC-FPGA platform QTS did not exhibit any malfunction, degradation of performance, deviation from specified operation, or beyond the tolerances indicated in the individual equipment or subsystem specification during tests.
- The tests did not cause damage to or failure of any components of the HFC-FPGA QTS.
- The HFC-FPGA platform QTS did not exceed allowable equipment emission limits as specified in RG 1.180 for conducted and radiated emissions.
- The HFC-FPGA platform QTS operated as intended during and after application of the EMI/RFI test levels as specified in RG 1.180 for conducted and radiated susceptibility.
- Evaluation of normal HFC-FPGA platform QTS operating performance data (inputs, outputs, and diagnostic indicators) demonstrated operation as intended.
- The EMI/RFI emissions did not cause the discrete I/O states to change.
- Analog I/O levels had accuracy within ±0.1% of span over the entire range.
- The self-diagnostic data indicated correct operation of the QTS.

The NRC staff reviewed Appendices C through E of the HFC-FPGA Equipment Qualification Summary Test Report and determined that the tested HFC-FPGA QTS met all acceptance criteria for EMI/RFI emission and susceptibility, ESD, SWC, and EFT tests and was qualified for operation up to the above tested limits applied to the HFC-FPGA QTS.

Licensees using the HFC-FPGA platform equipment in safety-related systems in NPPs must determine that application specific EMI/RFI, ESD, SWC, and EFT requirements do not exceed the capabilities of the HFC-FPGA system as evaluated in this SE. This determination and the suitability of the HFC-FPGA platform for a particular application are the responsibility of the licensees (see PSAI 5.2.5).

3.4.4 Seismic Stress Qualification

The seismic stress qualification testing of the HFC-FPGA QTS was performed to demonstrate compliance with criteria and guidance in RG 1.100, its endorsed IEEE Std. 344-2004, and relevant guidance in EPRI TR-107330. The seismic stress test was conducted to show specifically that the physical components on the HFC-FPGA QTS remain in place and operational during and after application of significant inertial forces during tests. The overall objective of the seismic stress qualification testing is to demonstrate the suitability of the HFC-FPGA platform to be used as a seismic Category 1 safety device.

RG 1.100 describes methods that the NRC staff considers acceptable for use in seismic stress qualification of electrical and active mechanical equipment. This regulatory guide provides an endorsement of IEEE Std. 344-2004 with exceptions and clarifications.

Clause 5 of IEEE Std. 344-2004 states, in part, that “The seismic qualification of equipment should demonstrate an equipment's ability to perform its safety function during and/or after the time it is subjected to the forces resulting from one Safe Shutdown Earthquake (SSE). In addition, the equipment must withstand the effects of a number of Operating Basis Earthquakes (OBEs) prior to the application of a Safe Shutdown Earthquake (SSE).”

An OBE is a seismic event during which all equipment necessary for continued plant operation without undue risk to the health and safety of the public is required to remain functional. An SSE is the maximum considered earthquake in the design of a NPP and the earthquake for

which structures, systems and components (SSCs) important to safety are designed to remain functional.

RG 1.61, Rev. 1 establishes evaluation guidance for applicants and licensees regarding the acceptable damping values to be used in the elastic dynamic seismic analysis and design of SSCs, where energy dissipation is approximated by viscous damping. Section 4.3.9 of EPRI TR-107330 provides additional guidance for establishing seismic withstand requirements for digital protection systems.

Prior to performing the OBE and SSE tests, a resonance search was conducted to confirm no abnormalities in the HFC-FPGA QTS structure or mounting and to identify any resonance response frequency within the test spectrum. If one or more resonance frequencies are identified, the test spectrum shall be centered on the frequency having the greatest response. The test results show that no adverse response was detected, and no resonance frequency was found during the search. The resonance search process passed all acceptance criteria as specified and the HFC-FPGA QTS was determined to be rigid.

Both Section 8.2.4.5 of the Amendment for HFC-FPGA system of HFC-6000 safety platform TR and Appendix F of the HFC-FPGA EQ summary test report specify the seismic qualification requirements to be five triaxial OBE tests conducted in succession at 5% damping followed by one triaxial SSE test conducted at 5% damping. These requirements are for seismic Category 1 safety systems.

The maximum acceleration for SSE and OBE levels shown in Figure 4-5 of EPRI TR-107330 are 14 g and 9.75 g, respectively, at frequencies greater than 3 Hz, based on 5% damping. Since the HFC-FPGA platform design is generic, there is no plant specific SSE or OBE acceleration level with which to evaluate and compare test results with. Instead, as presented in both the HFC-FPGA safety platform TR and the HFC-FPGA Equipment Qualification Summary Test Report, HFC used a seismic test spectrum which is very similar to Figure 4-5 of EPRI TR-107330 as the seismic envelope to qualify the HFC-FPGA platform QTS. To demonstrate that the HFC-FPGA platform QTS meets the requirements for seismic Category 1 safety equipment, the representative HFC-FPGA QTS was subjected to accelerated aging, by performing five OBE tests in succession, followed by a seismic stimulation test representing the SSE condition. However, licensees using this HFC-FPGA platform must ensure that their plant-specific in-equipment response spectra are enveloped by the seismic test spectrum qualification envelope used for the HFC-FPGA platform QTS (see PSAI 5.2.5).

Seismic stress tests were performed at the ETL facility in Dallas, Texas. The HFC-FPGA QTS test chassis was the same one that was used during other EQ tests. The NRC staff reviewed the equipment test subject component list as well as the modules under test layout configurations, documented in the HFC-FPGA Equipment Qualification Summary Test Report, and confirmed that a reasonable representative configuration was employed for the HFC-FPGA platform. The NRC staff also confirmed that all HFC-FPGA platform modules identified above in this Section 3.4 are included in the QTS and were thus subjected to the seismic qualification tests performed.

A summary of seismic test results was provided in Appendix F of the HFC-FPGA Equipment Qualification Summary Test Report. Resonance search tests confirmed no abnormalities in the HFC-FPGA QTS cabinet or component structures. Chassis and module physical integrity and correct functional operation of the QTS were verified before, during, and after excitation. The NRC staff reviewed the seismic test specifications defined in the HFC-FPGA EQ test plans and

procedures and confirmed the acceleration levels to be consistent with HFC-FPGA cabinet and module specifications identified in Section 8.0 of the HFC-FPGA platform TR and its Qualification Summary Test Report. The NRC staff reviewed the HFC-FPGA seismic test results and confirmed that the seismic acceleration levels to which the representative platform modules were tested met the seismic resistance specifications for the HFC-FPGA platform as provided in Section 8.0 of the HFC-FPGA Platform Topical Report.

In summary, the seismic stress qualification testing results for the HFC-FPGA QTS show that:

- Seismic testing of the HFC-FPGA QTS was performed in accordance with the criteria in RG 1.100, its endorsed IEEE Std. 344-2004, and related guidance in EPRI TR-107330.
- The HFC-FPGA QTS met all applicable performance requirements during and after application of the seismic test vibration levels.
- Results of the operability tests performed after seismic testing show that exposure to the seismic test conditions had no adverse effect on the HFC-FPGA QTS performance.
- The seismic test results demonstrate that the HFC-FPGA platform is suitable for qualification as seismic Category 1 equipment.
- The seismic test results demonstrate that the representative module mounting configuration used during testing is adequate to support seismic qualification of HFC-FPGA based safety systems.

Based on review of the HFC-FPGA seismic test results, the NRC staff determined that the platform QTS satisfies the guidance and criteria on seismic qualification in RG 1.100, its endorsed IEEE Std. 344-2004, and EPRI TR-107330. The NRC staff finds that seismic qualification of the HFC-FPGA platform QTS has been acceptably demonstrated for five OBE tests in succession at 5% damping and one SSE test up to acceleration levels shown in the OBE and SSE test spectra in the HFC-FPGA Platform Topical Report and its Equipment Qualification Summary Test Report. However, the use of HFC-FPGA platform modules for the performance of safety system functions in a NPP requires licensees to determine that plant-specific seismic requirements do not exceed the seismic withstand capabilities tested for the HFC-FPGA platform QTS. A plant using the HFC-FPGA platform is therefore required to establish plant specific seismic criteria for an HFC-FPGA based system.

From all the above evaluations, the NRC staff confirmed that the platform QTS operated normally during and following all qualification tests. The NRC staff finds that the HFC-FPGA EQ testing results show that the HFC-FPGA QTS met all the acceptance criteria specified for pre-qualification tests, operability tests, prudency tests, qualification tests (environmental, EMI/RFI, ESD, SWC, Class 1E to Non-1E isolation, and seismic), and post-qualification tests. Therefore, the NRC staff concludes that the HFC-FPGA platform modules evaluated in this SE could be used as safety-related equipment.

3.5 HFC-FPGA Platform Integrity Characteristics

SRP Chapter 7, Appendix 7.1-C, Section 5.5, “System Integrity,” states that a special concern for digital computer-based systems is confirmation that the real time performance of the system is adequate to ensure completion of protective actions within the critical time periods identified within Clause 4.10 of IEEE Std. 603-1991. SRP BTP 7-21, “Guidance on Digital Computer Real-Time Performance,” provides supplemental guidance to evaluate the real-time performance of digital systems and discusses the identification of bounding real-time performance specifications and the verification of these specifications to demonstrate real-time performance. The establishment of predictable performance and behavior for a platform supports the future evaluation of a safety system that is based on the platform. The following sections describe performance capabilities of the HFC-FPGA platform.

3.5.1 HFC-FPGA platform Response Time

Applicable Criteria for Response Time performance:

- 10 CFR 50 Appendix A, GDCs 20, 21, 23, and 25
- SRP BTP 7-21
- 10 CFR 50.55a(h)
- IEEE Std. 603-1991
- 10 CFR 50.36(c)(1)(ii)(A)

Section 6.7 of the HFC-FPGA platform TR (References 2 & 3), “Deterministic Performance Conclusion” describes platform timing performance characteristics. Response times for an HFC-FPGA platform-based safety system are determined by two factors.

The first factor is the duration of application logic processing. The response time of application logic processing is dependent on application characteristics such as the complexity and number of logic blocks that are implemented on the FPGA module. Once established, the application logic response times become deterministic and are based on the established design characteristics of the application.

The second factor of response time is the communication between the FPGA controller modules and the I/O modules over the F-Link interface. The F-Link interface is designed to function in a deterministic manner. This is accomplished by an established F-Link cycle that uses a fixed cycle time and data packet structure. Furthermore, the HFC-FPGA platform includes self-diagnostic features that detect communications errors on the F-Link interfaces such that non-deterministic performance over this link is identified and addressed accordingly by the system. These diagnostic features are designed to initiate alarms and cause system outputs to enter fail-safe states when defined conditions are met. The HFC-FPGA failure modes and effects analysis (Reference 10) includes analysis of platform failure modes that affect deterministic system performance. Section 3.3.2.5 of this SE includes an evaluation of the HFC-FPGA FMEA.

Thus, once an HFC-FPGA-based system is initialized and placed into operation the internal modules of that system operate on a fixed duration cycle which is not dependent on the logic functions performed. The response time characteristics of the resulting safety functions are deterministic because they are predictable, not variable, repeatable, and measurable. However, the establishment of that fixed duration cycle time and determination that the established duration and cycle frequency will meet plant specific timing requirements remains a

plant application specific activity. Each licensee must therefore determine that HFC-FPGA-based system response time characteristics are suitable for its plant-specific application. See PSAI 5.2.4.

3.5.2 HFC-FPGA Determinism

Criteria for evaluation of deterministic performance characteristics of the HFC-FPGA platform were derived from the following:

- 10 CFR Part 50, Appendix A, GDC 21, “Protection system reliability and testability”
- SRP Chapter 7, Appendix 7.1-C, Section 6.1, “Automatic Control”
- SRP BTP 7-21
- EPRI TR-107330, Section 4.4.1.3, “Program Flow Requirements”

HFC-FPGA system control processes are performed by the systems controller modules in accordance with defined deterministic logic execution cycles of the module control FPGA. The control FPGA initiates all HFC-FPGA functionality including communication, application logic processing, and I/O control. Section 6.1 of the HFC-FPGA platform TR (References 2 & 3) describes the basic operation of the centralized controller module and Section 6.2 describes the basic operation of the system I/O modules.

The HFC-FPGA system is designed to have a predetermined maximum response time for performing safety functions. Performance of HFC safety functions includes (1) processing of input signals, (2) communication with I/O modules over the F-Link and (3) performing application logic processing.

Processing of I/O signals is performed by the HFC I/O modules which operate on a fixed timing cycle that is determined by the logic of the control FPGA within each module.
Information is provided from input modules to the processor module and from processor module to output modules via the F-Link backplane communication interface. The communication component of system deterministic performance is accomplished by the F-Link cycle which uses a fixed cycle time and a fixed data packet structure.

The time required to perform application processing is dependent on plant specific application logic design however, once established, this time becomes fixed. Therefore, if application logic does not change during system operation, the safety function time response of the HFC system remains constant.

The method used by HFC to establish deterministic system performance provides assurance that each consecutive process is completed prior to initiation of the next cyclic process. The HFC-FPGA controller design does not include the use of interrupts. System logic is executed in accordance with pre-defined logic configurations and all logic functions are completed during each work cycle of the system FPGA’s. Initiation of subsequent logic execution cycles occurs only upon completion of the previous logic execution cycle. Each HFC-FPGA performs assigned logic functions independently of all other FPGAs in the system and therefore operates at a known deterministic periodic rate. The resulting response time characteristics of the safety functions are deterministic because they are predictable, and not variable, and because they are repeatable, and measurable.

The NRC staff determined that design features, operation of the HFC-FPGA system, and HFC’s commitments to perform timing verification tests provide adequate assurance that HFC-FPGA

based safety systems will operate deterministically to meet the criteria of BTP 7-21 and is therefore acceptable.

3.5.3 Platform Diagnostics

The HFC-FPGA platform includes self-diagnostic capabilities that are summarized in Section 6.3 of the HFC-FPGA platform TR. The diagnostics functions of the HFC-FPGA controller and I/O FPGA Processing Unit (FPU) are accomplished in three categories: (1) power on diagnostics, (2) continuous DIAG block diagnostics, and 3) board operational diagnostics.

3.5.3.1 Power on Diagnostics

Power on diagnostics run every time a Controller or platform I/O module is energized or if the module reset switch is actuated. The power on diagnostics use data obtained from the Serial Peripheral Interface flash memory to determine that the module has been configured properly and that communications are functioning properly with the connected FPGA.

3.5.3.2 Continuous DIAG Block Diagnostics

All HFC-FPGA controllers and I/O modules contain a DIAG block that runs continuous diagnostics. In addition to the continuous diagnostics, the process scheduler periodically executes the diagnostic checking function as required for the architecture in which the diagnostics are running. This loop begins after successful completion of the initial tests and continues unless an over-voltage is detected, under-voltage is detected, or timeout occurs during one of the diagnostic check functions.

When the DIAG block detects over-voltage, the DIAG block forces the board to transition to the fail-safe state. Under-voltage detection suspends block processing, and if resolved, moves the module back to the DIAG reset and initialization states. Diagnostics do not function while the under-voltage condition is present. Timeout occurs if one of the diagnostic checking functions fails to complete within a pre-defined time. This transition suspends the diagnostic loop and initiates a restart of the heartbeat sequence with the mate FPGA over the HPI using semaphores.

3.5.3.3 Board Operational Diagnostics

Diagnostic FPGA Architecture **-** Each module of the HFC-FPGA platform contains a control FPGA which performs the system safety functions as well as a separate diagnostic FPGA which is used to monitor Control FPGA operation. The control and diagnostic FPGAs communicate with one another through an HPI communications interface.
Upon detection of excess errors in communication, application, or I/O processing, the Diagnostic FPGA can be configured to initiate the following failsafe actions:

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

Additional information on Diagnostic FPGA processing functions is provided in Section 5.3.2 of the HFC-FPGA platform TR.

Input signal comparison - For input modules, both Control and Diagnostic FPGAs receive the same input channel data on the same hardware paths. This input is formed into scan data

which is compared via the HPI. If no errors are identified, the data is sent via F-Link to the controller module.

Output Data Verification - For output modules, output data is received from the controller module via the F-Link by both the Control and the Diagnostic FPGAs. The two FPGAs then exchange their data to verify that both have received the same data. If there is a discrepancy between the two, then the data is rejected as invalid.

Power Supply Monitoring - Control and Diagnostic FPGAs are designed to perform power supply diagnostics in a cross-monitoring configuration. The Control FPGA monitors the power supply voltages of the Diagnostic FPGA and the Diagnostic FPGA monitors the power supply voltages of the Control FPGA. This diagnostic is used to confirm that the FPGAs have healthy power supplies which are essential for proper system operation.

Cyclic Redundancy Check (CRC) Memory Check - Data in the Dual Port Memory (DPM) and Two Port Memory (TPM) is stored with a CRC that can be used to verify the quality of the data stored. All application related memory spaces used in process control are protected by CRC-16. When data in memory is changed, the CRC-16 data checksum value is re-generated. If a CRC error is detected, an alarm may be generated, and the module can be placed into a fail-safe state. The HFC-FPGA platform can detect memory corruption by checking application results using Control/Diagnostic FPGA Transmit message CRC compare over the HPI interface.

Diagnostic State Check - Diagnostic state checking is performed within the HFC modules using messages within pre-defined memory locations in the diagnostic block DPM. This allows control and diagnostic FPGAs to share diagnostic process state through coded messages. This diagnostic is used to coordinate the checking functions of the FPGAs and to provide assurance that diagnostic functions are being performed as designed.

Watchdog Mechanisms **-** The HFC-FPGA platform uses three types of watchdog mechanisms to detect system faults. They are:

- Reset Generator Watchdog
- Heartbeat Sequence Watchdog
- Application Processing Watchdog.

Reset Generator Watchdog - The HFC-FPGA platform design includes a hardware watchdog circuit that generates a power up reset signal, performs watchdog monitoring of the diagnostic FPGA and provides a manual push button FPGA reset capability.

During module operation, the Diagnostic FPGA prevents the watchdog timer from timing out by sending continuous reset pulses to the reset generator circuit. The reset pulses are derived from the Diagnostic FPGA main clock. If the reset pulse signal is absent for a pre-defined period, the reset generator will reset both the Control and Diagnostic FPGAs. The NRC staff notes that there is no hardware watchdog circuit or reset generator for the Control FPGA. This is however acceptable because by monitoring the functionality of the Diagnostic FPGA, the design is ensuring that Control FPGA functions are continuously monitored by the Diagnostic FPGA. As such, a failure of the Control FPGA such as a clock malfunction would be detected by the Diagnostic FPGA to assure both annunciation and fail-safe actuations are initiated.

Application Processing Watchdog - The application processing watchdog function detects failures of either application processing or process scheduler functions. The application processing function is dependent on the process scheduler function to operate so a failure of

either will cause the application watchdog function to time out. If the application processing watchdog fails to detect activity of the application processing function for a configurable time period, it will cause the module to transition to a fail-safe state. Loss of application activity is triggered if either of the following events occur:

- Application processing starts and does not complete in the specified time period
- After the completion of application processing, new application processing fails to start within the specified time period.

Heartbeat Sequence Watchdog - Communication between the control and diagnostic FPGAs through the HPI is used as a means of continuously verifying FPGA operation. Heartbeat checking uses a coded sequence of values that are transferred and checked over the HPI. Failure to correctly control or to detect the heartbeat sequence values in HPI transfers will cause the module to transition to a failsafe state. Determination of fail-safe states for a safety function is a plant application specific activity. Therefore, a licensee referencing this TR should specify fail safe states for all system actuation output signals. This is PSAI 5.2.13.2.

The HFC-FPGA diagnostic functions described above can be used to support compliance with GDC 21. However, determination of full compliance with these criteria is dependent on the specific safety system design as well as the plant specific safety functions performed by the system. Therefore, determination of GDC 21 compliance is a plant-specific evaluation item. See PSAIs 5.2.2, 5.2.13.1 and 5.2.13.2.

The NRC staff found that HFC-FPGA diagnostic functions can address system failures by identifying expected failures and by providing the capability to annunciate such failures to the operator. The NRC staff also found that platform diagnostics do not adversely affect channel independence or system integrity.

A combination of diagnostic tests, periodic tests, and surveillance activities are necessary to successfully detect failures and support effective maintenance of an HFC-FPGA based system for a plant specific application. Periodic surveillance tests must be performed to detect failures or problems that are not detectable by platform diagnostic functions. Maintenance activities including periodic surveillance testing will be defined based on plant-specific application requirements. In addition, methods of failure management must be defined for a plant-specific application. See PSAIs 5.2.13.1 and 5.2.13.2.

3.6 Setpoint Determination Methodology

The HFC-FPGA platform TR states that "*setpoint control for the HFC-FPGA system is designed such that the setpoints for nuclear plants can be maintained considering anticipated operating transient and postulated accident conditions.*" The NRC staff determined that measurement uncertainties associated with the HFC-FPGA platform equipment will need to be considered and factored into the setpoint methodology being used by a licensee installing an HFC-FPGA based system.

The contribution of the HFC-FPGA platform to setpoint uncertainty must be addressed in an application-specific analysis. Since the TR does not include a specific setpoint methodology to be used to support setpoint determination activities, no evaluation of a HFC-FPGA platform specific methodology was performed. An analysis of accuracy, repeatability, thermal effects, and other necessary data for use in determining the contribution of the HFC-FPGA platform to instrumentation uncertainty must be performed as PSAI 5.2.11.

3.7 Diversity and Defense-in-Depth

Diversity and Defense-In-Depth (D3) is a strategy that is applied to the overall I&C system architecture in the context of a specific plant design. Section 6.10 of the HFC-FPGA platform TR describes a prospective plant-specific analysis approach that is derived from NUREG/CR-6303. The key assumption in this analysis is that all systems using the HFC-FPGA based platform will be subject to a common-cause failure (CCF) and the safety functions implemented on those systems will be disabled by such a fault. Furthermore, the HFC-FPGA platform design does not contain design features that would provide platform level diversity. Therefore, no evaluation of HFC-FPGA platform diversity was performed by the NRC staff.

HFC describes safety system design approaches that can be used to address potential CCF vulnerabilities of the HFC-FPGA platform. However, the degree to which these prospective design options provide mitigation of CCF cannot be assessed outside of the application-specific context. Thus, the performance of a plant specific D3 analysis is a plant specific action for safety-related applications of the HFC-FPGA platform. See PSAIs in Section 5.2.13.

3.8 HFC-FPGA Communications

The communications interfaces for the HFC-FPGA platform are described in Section 3.2.3 of this SE. The deterministic characteristics of the communication functions provided by the HFC-FPGA platform are described in Section 3.5.2 of this SE.

Digital I&C (DI&C)-ISG-04 contains NRC staff positions on three areas of interest: (1) interdivisional communications, (2) command prioritization, and (3) multidivisional control and Display Stations. An analysis of HFC-FPGA platform conformance to DI&C-ISG-04, Revision 1 was provided in Section 6.9.2 of the HFC-FPGA platform TR (References 2 & 3). The HFC-FPGA platform is not designed to perform command prioritization functions and does not use multidivisional control and display stations or communications between safety divisions. Therefore, the NRC DI&C-ISG-04 evaluation scope only addresses criteria for communications to external systems.

Because the HFC-FPGA platform TR (References 2 & 3) does not address specific applications or establish a specific safety system design, evaluation is limited to consideration of the means provided within the platform to address issues related to interactions among safety divisions and between safety-related equipment and equipment that is not safety-related. The following subsections provide an evaluation of HFC-FPGA platform level communications to applicable DI&C-ISG-04 criteria. PSAI 5.2.14 is included in this SE to address system level compliance to DI&C-ISG-04.

3.8.1 DI&C-ISG-04, Section 1 – Interdivisional Communications

Interdivisional communication is not allowed and is not part of the HFC-FPGA architecture. However, the HFC-FPGA platform contains interfaces that support communication between the safety system and external non safety-related systems. The guidance of ISG-04 Section 1 applies to the safety to non-safety interfaces. The following 20 points of DI&C-ISG-04 Section 1 were used to evaluate the HFC-FPGA platform safety to non-safety communications.

Interdivisional Communications, Point 1:
The HFC-FPGA platform includes several types of communication interfaces which are described in Section 3.2.3 of this SE. Among these interfaces are the G-Link and C-Link interfaces that together can be used to establish communication links between platform controller modules and external systems such as an engineering workstation or a plant computer system.

The HFC-FPGA platform described in the TR includes capabilities to comply with the guidance provided in Staff Position 1, Point 1. For example, the controller modules operate independently from the gateway modules. The gateway modules also have diagnostic capabilities to monitor the status of its communication interfaces. These communications diagnostics can identify loss or corruption of communication data which is required to support safety functionality. A loss or corruption of data can therefore be addressed by application logic to retain the ability of the safety system to perform safety functions without reliance on external data.

The NRC staff recognizes that the HFC-FPGA platform includes system design features that could be used to establish compliance with the guidance provided by Staff Position 1, Point 1. However, evaluation of this point will require plant application specific analysis to verify compliance with this staff position. See PSAI 5.2.14 for plant specific actions pertaining to DI&C-ISG-04.

Interdivisional Communications, Point 2:
To address this criterion, the NRC staff evaluated the G-Link and C-Link interfaces, which can be used to provide communications between the HFC-FPGA controllers and non-safety-related systems. The HFC-FPGA platform TR states that C-link does not communicate with any outside division.

The G-Link interfaces are used to support communications between the HFC controller modules and gateway modules. Both modules are safety related and both reside within the same safety division of the system. Therefore, this interface is considered intra-divisional and the criteria of ISG-04 do not directly apply. However, these interfaces provide a communications pathway to external systems through gateway module C-Link interfaces. The G-Link interfaces also include communication independence and diagnostic features described in Sections 5.1.4 and 6.6 of the HFC-FPGA platform TR. Relevant G-Link communications features are listed below:

- The G-Link is a dedicated communication path between the redundant HFC controllers and the Gateway Controller module.
- Platform I/O modules do not contain G-Link Interfaces.
- G-Link communication is separate and electrically isolated from F-Link Communication.
- Data validation is performed using cyclic redundancy checks (CRC).
- Data is transferred using dual port memory blocks.
- The Controller Diagnostic FPGA controls the G-Link transmit enable signal.
- The Controller Diagnostic FPGA can prevent the G-Link data packet transmission.
- All G-Link messages are passed directly from sending node to receiving node without the involvement of equipment outside the division.
- The G-Link uses a token-passing communication protocol, in which token passing occurs in a defined sequence.
- The G-Link token passing design prevents excessive communication of data.
- The Controller Diagnostic FPGA performs a comparison of G-Link Data with Control FPGA and identifies mismatch of data as a diagnostic error.

- Loss of G-Link function does not impact the ability of the system to perform safety functions.

The C-Link interface is a one-way broadcast communications path from the safety-related Gateway module to external systems. The TR describes C-Link data communication as a one-way interface that will be enforced at the application level. Because this interface is intended to prevent data communication to the safety system, there is no potential for C-Link communications to inhibit or delay the safety functions being performed by the controller modules of the system. C-Link is only used in gateway modules and is not present on the HFC-FPGA I/O or control modules.

The means of enforcing one-way communications through the C-Link interfaces is provided by the gateway application and involves the use of HFC proprietary UCP (Universal Communication Protocol) which is a broadcast protocol. The Gateway module initiates C-Link communications by sending broadcast messages to the associated interfaces. External devices, such as an engineering workstation or a plant computer system, then receive broadcast data from the Gateway module through the C-Link interface.

The NRC staff also notes; the HFC-FPGA platform can be configured to support data input from the C-Link if it is allowed by the requirements of the application. This type of communication is not within the scope of the HFC-FPGA platform TR and is therefore not evaluated in this SE. Applications that allow this type of communication through the C-Link must provide an alternative means of establishing communication independence. See PSAI 5.2.14 for additional plant specific actions that would be required for such a configuration.

The NRC staff determined that HFC-FPGA safety system chassis can be protected from adverse influences caused by information or signals originating from the C-Link. The NRC staff recognizes that the HFC-FPGA platform provides allowances for implementation of system features that could meet the guidance criteria provided by Staff Position 1, Point 2. However, evaluation of this point will require plant application specific analysis to verify compliance with this staff position. See PSAI 5.2.14 for plant specific actions pertaining to DI&C-ISG-04.

Interdivisional Communications, Point 3:
The HFC-FPGA platform can be configured to support data input from outside of the assigned safety division via the C-Link if it is allowed by the requirements of the application. This type of communication is not within the scope of the HFC-FPGA platform TR and is therefore not evaluated in this SE. Applications that allow this type of communication through the C-Link must provide an alternative means of establishing communication independence. See PSAI 5.2.14 for additional plant specific actions that would be required for such a configuration.

Interdivisional Communications, Point 4:
The HFC-FPGA platform TR states that C-link does not communicate with any outside division however, communication with non-safety-related devices is supported by the platform design. The HFC G-Link communications interface uses separate and independent communication logic blocks to manage external communication related tasks for the controller module FPGAs. This communication logic is separate from the FPGA application logic that performs system safety functions. The safety function FPGA logic on the controller FPGA does not perform communication related functions other than to transfer data to and from a dual port memory logic block within the FPGA.

The HFC-FPGA platform uses an alternative method to the shared memory between distinct processing devices method described in ISG-04. This alternative method provides communication processing logic that is separate from safety function processing logic but resides in a common physical device, the FPGA, in each controller module. In lieu of a separate shared memory resource, this alternative method uses Dual Port Memory IP logic blocks to create a data transfer path within each FPGA device. This provides data exchange to safety logic functions in a manner that ensures a deterministic completion of each safety function.

All of the HFC-FPGA platform application logic circuits are developed as safety-related, which meets Point 4's guidance that safety function processors, communications processors, the data exchange memory resource, supporting circuits, and programming be developed as safety-related. Additionally, the use of IP cores within the HFC-FPGA design was analyzed by HFC and was determined to meet requirements for safety-related equipment. See Section 3.2.4 of this SE for additional information on the use of IP cores in the HFC-FPGA design.

The HFC-FPGA platform DPM IP cores allow non-intrusive exchange of data with the safety function logic circuits so a failure of the DPM logic for G-Link communications cannot adversely affect the performance of the safety function processing. The HFC-FPGA FMEA, which is evaluated in Section 3.3.2.5 of this SE includes G-Link interface failure modes. This analysis determined that such failures do not adversely impact safety function logic processing capabilities of the system.

The NRC staff determined the HFC-FPGA platform communication method, which

- produces communication processing logic circuits that are separate from safety processing logic circuits but reside in a common physical FPGA device and
- includes data exchange paths within the FPGA that ensure a deterministic completion of each safety function is an acceptable alternative to the implementation method provided in ISG-04 Point 4. The alternative method supports a deterministic completion of each safety function without adverse effect from the communication processing.

The NRC staff determined the HFC-FPGA controller modules support meeting the criteria of Point 4 using an alternative method. The NRC staff further determined plant specific actions are necessary to ensure that plant specifications document the safety analysis that applies to its safety function determinism and that plant specific implementation, V&V, and testing efforts demonstrate these safety functions will be performed within the established safety design bases timeframes.

Interdivisional Communications, Point 5:
The HFC-FPGA platform provides an alternative approach to shared memory access, wherein communication logic circuits non-intrusively transfer safety function data using DPM IP blocks and communication activities cannot delay or otherwise adversely affect the performance of safety functions. The HFC-FPGA platform also includes diagnostic functions that are designed such that failures of the system to meet timing requirements will activate a system alarm, halt safety function operation and force the system outputs to pre-defined fail-safe states.

The NRC staff determined the HFC-FPGA platform communication interfaces support compliance with the criteria of Point 5 because the platform includes fault detection functions and alarm logic to respond to a system's failure to meet its plant specific limiting cycle time. Each HFC-FPGA safety application will have a set cycle time that is dependent on the specific application. The NRC staff further determined plant specific actions are necessary to ensure

plant specifications meet the criteria of Point 5 with respect to detection of and initiation of an alarm for cycle time performance in excess of the limiting cycle time. See PSAI 5.2.14 for plant specific actions pertaining to DI&C ISG-04.

Interdivisional Communications, Point 6:
The NRC staff determined the HFC-FPGA platform G-Link communication components, which are used for all communications between HFC controller safety function logic and external systems through the gateway module, meet the criteria of Point 6 because safety function logic circuits do not perform communication handshaking and do not accept communication related interrupts.

Interdivisional Communications, Point 7:
The HFC-FPGA platform uses defined message structures for transfer of data over the communication pathways. Data not conforming to this structure is rejected and error flags are set upon such occurrence. Communication is performed in accordance with the HFC proprietary UCP (Universal Communication Protocol) used by the G-Link and C-Link interfaces. Based on the review of HFC-FPGA platform communications interfaces and protocols, the NRC staff determined that HFC-FPGA communication methods meet the criteria of point 7.

Interdivisional Communications, Point 8:
The NRC staff reviewed communications protocols used for data exchanged over the HFC G-Link and C-Link interfaces, described in Section 5.1.4 of the HFC-FPGA platform TR and determined that dedicated communication logic circuits are used to manage data transfers in a manner, which cannot adversely impact safety functions performed by the safety logic. Determination of communications interconnections between a safety system and nonsafety systems is a plant application-specific activity. The base platform architecture identified in the TR does not specify any direct connections or bi-directional communication between the HFC-FPGA and other non-safety-related systems. However, the TR does identify the capability for one-way communication from the gateway module to non-safety-related components across the C-Link network.

To ensure independence, HFC established a design principle for nuclear safety applications that restricts communication over the C-Link network to broadcast-only messages.
The base architecture presented for the HFC-FPGA platform is representative of a single division in a safety system and does not include communication interfaces between different safety divisions. Communications interconnections established between a safety division and other safety-related equipment in a plant are therefore dependent on the safety system design. The NRC staff determined that methods used by the HFC-FPGA platform for conducting data exchange between safety divisions and between safety and non-safety-related systems are consistent with the criteria of Point 8. However, implementation of the methods described in the HFC-FPGA platform TR for establishing communications to external systems is a plant specific activity. See PSAI 5.2.14 for plant specific actions pertaining to DI&C ISG-04.

Interdivisional Communications, Point 9:
The alternative method described in Staff Position 1, Point 4 above uses separate FPGA logic units to provide dedicated pre-specified physical memory locations within the FPGA to store message data and to segregate input data from output data. These pre-specified memory areas within the FPGA are not used for other purposes.
The NRC staff determined the HFC-FPGA platform alternative method of data sharing using dual and two port memory logic blocks provides an acceptable means of meeting the guidance

in Point 9. The NRC staff determined the HFC-FPGA platform meets the criteria of Point 9, as applied to FPGA technology.

Interdivisional Communications, Point 10:
The HFC-FPGA platform logic cannot be modified during system operation because the programming ports used to modify system module FPGA logic are normally inaccessible. To modify system logic designs, the associated module must be removed from the chassis to allow access to the programming ports on the module circuit board and a specialized connector must be used. Removal of the logic module from the system chassis also causes all system outputs to change to pre-defined fail-safe states and actuates a system alarm.

HFC-FPGA engineering workstation cannot be used to alter addressable constants, setpoints, parameters, and other settings associated with a safety function during system operation because the engineering workstation is only connected to the safety system through the C-Link interface which is configured to be one-directional. Changes to system addressable constants, setpoints, parameters, and other settings can therefore only be made when the safety system is inoperable.

The NRC staff determined the HFC-FPGA platform design meets the criteria of Point 10, because the platform's maintenance communication architecture prevents alteration of safety system logic and tuning parameters during system operation by way of a hardware disconnect. The NRC staff determined that the Point 10 criteria for physically restricting the capability of making tuning parameter changes to only one redundant safety division at a time are also met because there are no active communication interfaces that would allow transfer of data to the safety logic of any safety division during system operation.

Interdivisional Communications, Point 11:
The HFC-FPGA platform does not contain conventional software instructions or instruction sequences. Instead, the platform modules contain configured hardware logic circuits that are contained in the systems FPGA devices. Once a platform module has been programmed and placed into operation as a plant specific system, none of the available digital data communication interfaces supports alteration of the configured FPGA logic circuits. Information or messages received from external systems through G-Link interfaces cannot be used to control the execution of the safety division application logic and C-Link interfaces are configured to allow uni-directional communication to external devices.

The HFC-FPGA platform has monitoring and indication capabilities to alert operators when a safety division is bypassed or rendered inoperable. These design features detect and indicate when a system module is removed from the chassis to be reconfigured.

The NRC staff determined the HFC-FPGA platform meets the criteria of Point 11 because the platform has provisions that explicitly preclude changes the safety division logic circuits while the system is operable.

Interdivisional Communications, Point 12:
The platform TR describes three levels of defensive design that are used to ensure that safety functions executed by the HFC-FPGA system are unaffected by faults originating in non-safety equipment. These design features are as follows:

- One-way C-Link communications through the gateway module - The Gateway module is configured such that it is only able to broadcast data from the safety system to non-safety equipment.

- Redundant C-Link communication channels – The gateway module has separate network interface cards for each of the two redundant channels. The design of the C-Link Protocol contains a messages verification scheme and rules for synchronization to eliminate corrupt messages.
- G-Link Data Comparison - The HFC-FPGA controller modules compare the Glink data arriving form redundant gateway modules. Data is rejected if the messages do not match the pre-defined message structure, or each other.

HFC-FPGA system diagnostics are designed to detect and address faults in the C-Link and G-Link communication interfaces. These diagnostics monitor communications during system operation and can be used to actuate system alarms upon detection of a fault.

The HFC-FPGA FMEA (Reference 10) postulated communication faults for the G-Link interfaces. This analysis identifies how various faults are handled by an HFC-FPGA system. Because both G-Link and C-Link interfaces are redundant, a single fault does not affect interface operation. For each of the identified communications faults, the analysis identified a method of fault detection and determined that the effects of the fault on an HFC-FPGA system did not adversely affect the performance of required safety functions. The NRC staff therefore determined the HFC-FPGA platform design complies with Staff Position 1, Point 12.

Interdivisional Communications, Points 13 through 15:
As presented in the HFC-FPGA platform TR, F-Link and G-Link communications are not interdivisional. These interfaces are divisionally isolated, and a single failure of these interfaces does not disable safety system functionality. Other platform interfaces, (RIF, and HPI) are intra divisional interfaces for which the criteria of ISG-04 does not apply. As such, vital communications between safety divisions are not defined within the HFC-FPGA platform TR. Therefore, the NRC staff determined the criteria of Points 13, 14, and 15 are not applicable to the HFC-FPGA platform as presented in the TR.

If communication Interfaces are used to establish communications between safety divisions, then a licensee will need to perform an evaluation of these criterion during plant application development to ensure that an adequate level of independence between the safety divisions is established and maintained. See PSAI 5.2.14 for plant specific actions pertaining to DI&C ISG-04.

Interdivisional Communications, Point 16:
The NRC staff determined that only the C-Link interface is relevant to the criteria of Point 16 because all other platform interfaces are isolated within a single safety division. Because the C-Link is configured as a broadcast only one-way interface, the network connectivity, liveliness and real time performance characteristics of this interface cannot cause the safety functions of the HFC-FPGA system as implemented in the systems FPGA logic to stall, deadlock, or livelock. The NRC staff determined the HFC-FPGA platform meets the criteria of Point 16.

Interdivisional Communications, Point 17:
The HFC-FPGA platform TR defines conditions for EQ. All platform communication interfaces described in Section 3.2.3 of this SE were included in the HFC-FPGA platform qualification test specimen.

Only the C-Link interface is used for communication to systems external to the safety division. Qualification of C-Link components as established by platform qualification testing can therefore be used to demonstrate compliance with criteria of Point 17. However, as presented in the

HFC-FPGA platform TR, the C-Link is not used for communications that are vital to the safety functionality of a system.

If interfaces are used in a plant specific system design to establish vital communications between safety divisions, then a licensee will need to perform an evaluation during system development to ensure that associated components are qualified for anticipated normal and post-accident environments. See PSAI 5.2.14 for plant specific actions pertaining to DI&C ISG-04.

Interdivisional Communications, Point 18:
HFC-FPGA system hazard analyses activities are performed as part of the V&V processes used for platform and application development. A system hazard analysis is performed for each phase of platform and application design. Hazards associated with communication interfaces are included in these analyses. The NRC staff determined that platform hazard analyses and the requirement to perform plant specific failure modes and effects analyses per PSAI 5.2.9 satisfies the guidance provided in Staff Position 1, Point 18. See PSAI 5.2.14 for plant specific actions pertaining to ISG-04.

Interdivisional Communications, Point 19:
As stated in the HFC-FPGA platform TR, the communication protocol for C-Link, F-Link, and G-Link interfaces use a token passing method that occurs in a defined sequence. The NRC staff notes that only the C-Link interface is used for communication to systems external to the safety division therefore the criteria of Point 19 are only being applied to the C-Link. HFC determined that by using this token passing protocol, all nodes on a link have the capability to handle the maximum error rate calculated for a system.

The Token passing configuration is designed to prevent excessive communication of data over each link. The NRC staff notes that actual communication rates are plant specific. The design process includes provisions to ensure communication bandwidth does not adversely affect performance of safety functions. The TR also states that communication throughput thresholds and safety system sensitivity to communications throughput issues will be confirmed by testing on a plant specific basis. See PSAI 5.2.14 for plant specific actions pertaining to DI&C-ISG-04.

Interdivisional Communications, Point 20:
HFC evaluated HFC-FPGA response times for a generic safety application. The NRC staff determined the HFC-FPGA platform supports meeting the criteria of Staff Point 20. However, the plant specific design must be evaluated because this time will depend on the system configuration, plant application logic, and communication interfaces used. When implementing an HFC-FPGA safety system the licensee must perform a plant specific timing analysis and a validation test to verify that plant specific requirements for system response time presented in the accident analysis in the plants safety analysis report are met.

A discussion of the platform response time is provided in Section 3.5.1 of this SE. Each licensee must determine that HFC-FPGA-based system response time characteristics are suitable for its plant-specific application. See PSAIs 5.2.4 and 5.2.14 for plant specific actions pertaining to system response time verification and ISG-04.

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

The design of field device interfaces and the determination of means for command prioritization were not provided in the HFC-FPGA platform TR. If an HFC-FPGA platform-based design is

used for the development of a command prioritization system, then an additional evaluation of that system against the criteria of DI&C-ISG-04 Section 2 should be performed. Therefore, no evaluation against this staff position was performed. See PSAI 5.2.14 for plant specific actions pertaining to DI&C-ISG-04.

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

The HFC-FPGA platform includes non-safety engineering workstations to perform monitoring tuning of the system. Control over how the engineering workstations are used during operation is a PSAI. See PSAIs 5.2.12 and 5.2.14. Below is an evaluation of how the HFC engineering workstations can be used to meet the applicable guidance criteria.

Multidivisional Control and Display Stations, Point 1:
Non-safety engineering workstations use the C-Link for connectivity to the safety function processors. Because C-Link interfaces are configured for one-way communication to receive data from the HFC-FPGA through the gateway modules, no data can be sent from the non-safety EWS to the HFC-FPGA system. The non-safety EWS is therefore not capable of controlling operation of safety-related equipment. Communication to non-safety workstations meets the criteria of Point 1.

Multidivisional Control and Display Stations, Point 2:
Non-safety-related communications via C-Link was evaluated by the NRC staff was found to support compliance with the guidance provided for communications between safety and non-safety systems as discussed in Section **Error! Reference source not found.** of this SE. See PSAI 5.2.14 for plant specific actions pertaining to ISG-04.

Multidivisional Control and Display Stations, Point 3:
The HFC-FPGA platform does not include provisions for operation of safety-related equipment from non-safety-related workstations. Because non-safety systems are connected to the HFC-FPGA system through the one-way C-Link, they are not capable controlling operation of safety equipment. Therefore, the criterion of Point 3 does not apply to the HFC-FPGA system.

Multidivisional Control and Display Stations, Point 4:
The HFC-FPGA platform design does not include provisions for operation of equipment in other safety-related divisions. Therefore, the criteria of Point 4 do not apply to the HFC-FPGA system.

Multidivisional Control and Display Stations, Point 5:
The NRC staff determined that HFC-FPGA equipment is functionally independent from equipment in other divisions and from non-safety systems. In addition, HFC-FPGA safety systems do not perform non-safety control functions. Therefore, failures of platform equipment cannot affect the operation of equipment that is external to the safety system. The HFC-FPGA platform design is therefore compliant with the criteria of Point 5 however, compliance to plant safety analysis requirements remains a plant-specific criterion and must be addressed during application development. The NRC staff determined that the HFC-FPGA platform design features can be used to support compliance with the guidance of Point 5. See PSAI 5.2.14 for plant specific actions pertaining to DI&C-ISG-04.

3.9 Compliance to IEEE Std. 603-1991 and IEEE Std. 7-4.3.2-2003 Requirements

The determination and documentation of the design basis for a safety system is a plant-specific activity that is dependent on the system design. Since the HFC-FPGA platform TR does not include a specific application of the platform, the design basis for a safety system is not available for review and no evaluation of a platform application against these regulatory requirements could be performed. Nevertheless, the applicant provided a summary of compliance to the criteria of IEEE Standards 603 and 7-4.3.2 in Section 6.9.3, "Compliance with IEEE Standards" of the HFC-FPGA platform TR.

The HFC-FPGA platform TR states that HFC has applied the requirements of IEEE 603-1991, including guidance of RG 1.152, 1.153, and NUREG-0800, in the development of the HFC-FPGA modules. The HFC-FPGA platform therefore has design features that support compliance with IEEE Std. 603-1991 for a specific project.

The NRC staff reviewed Section 6.9.3 of the TR and evaluated the capabilities of the HFC-FPGA platform to address the criteria of IEEE Std. 603-1991 and IEEE Std. 7-4.3.2-2003. See PSAIs 5.2.15 and 5.2.16 for required plant specific activities.

3.9.1 Safety System Designation

Range of Conditions for Safety system Performance:
The platform TR establishes a qualified range of operation for an HFC-FPGA based safety system. Section 8.2.4, "Qualification Tests" of the HFC-FPGA platform TR documents details of equipment qualifications and provides references to specific qualification standards, test procedures and test reports that provide a basis for the platform component qualifications. This documentation can be used to support a plant specific application of the HFC-FPGA platform if plant specific environmental conditions do not exceed the established conditions to which the HFC-FPGA platform is qualified.

Functional Degradation of Safety System Performance:
The HFC-FPGA Platform design incorporates design features that establish independence between the safety system components of a safety system and non-safety-related systems connected via C-Link interfaces. See section **Error! Reference source not found.** of this SE for evaluation of communication interfaces between the HFC-FPGA system and non-safety related systems.

Reliability:
The HFC-FPGA platform TR (References 2 & 3) partially addresses this criterion by providing documented basis for platform self-diagnostic functions. HFC-FPGA platform self-diagnostic features are described in Section 5.3, "FPGA Software Architecture" of the TR and an evaluation of these platform features is provided in Section 3.5.3 of this SE.

Section 6.9.3 of the TR also partially addresses these criteria by providing predicted reliability values for HFC-FPGA modules. These values can be used by a licensee to support a reliability analysis to show compliance with plant specific reliability requirements. Section 3.3.2.66 of this SE documents the NRC staff's SE of the reliability characteristics of an HFC-FPGA platform-based safety system.

3.9.2 Safety System Criteria

The establishment of safety groups that can accomplish a given safety function is a plant specific activity and the TR scope does not include specific applications. Therefore, the NRC staff evaluations of the requirements of IEEE Std. 603-1991 Section 5 are limited to assessing capabilities and characteristics of the HFC-FPGA platform that are relevant to satisfy each requirement. See PSAI 5.2.15 for additional activities necessary to establish conformance with the requirements of IEEE Std. 603.

Clause 5 of IEEE Std. 7-4.3.2-2003 contains requirements to supplement the criteria of IEEE Std. 603-1991 Clause 5. In addition, SRP Chapter 7, Appendix 7.1-D, Section 5 contains specific acceptance criteria for IEEE Std. 7-4.3.2-2003 Clause 5.
The following clauses of IEEE Std. 603 were not evaluated because addressing compliance with this guidance is a plant-specific activity that depends on the system design.

- Clause 5.8, “Information Displays”
- Clause 5.11, “Identification”
- Clause 5.12, “Auxiliary features”
- Clause, 5.13, “Multi-unit stations”
- Clause 5.14, “Human Factors considerations”

Single Failure Criterion:
Since the HFC-FPGA platform TR does not address a specific application for approval, the evaluation of this requirement is limited to consideration of the means provided within the platform to address failures. The NRC staff evaluation of the capabilities and characteristics of the HFC-FPGA platform that are relevant to the single failure criterion are documented in Section 3.5.3, “Self-Diagnostics and Test and Calibration Capabilities,” and in Section 3.3.2.5, “Failure Mode and Effects Analysis,” of this SE.

To meet the single failure criterion, it is expected that the HFC-FPGA system would be applied to redundant process safety divisions and at least two trip logic trains for each RPS or ESF actuation function. These redundant divisions and trains are required to be electrically isolated and physically separated. Qualified isolation devices must also be used to ensure functional operability of the safety system when subjected to physical damage, short circuits, open circuits, or credible fault voltages on the device output terminals. The results of the FMEA performed for the HFC-FPGA platform found that all component failures that could affect unit performance are detectable. Section 3.3.2.5 of this SE provides additional FMEA evaluation information. Single failure criterion at the system level will need to be evaluated during plant application development. See PSAI 5.2.9 for additional information on this plant specific activity.

IEEE Std. 7-4.3.2-2003 does not include criteria beyond those identified in IEEE Std. 603-1991 for Single Failure Criteria however, IEEE 7-4.3.2-2016 does include additional criteria. The NRC staff therefore reviewed HFC-FPGA platform design conformance to the criteria within the current version of this criteria.

The NRC staff determined that an HFC-FPGA platform-based safety system can be configured to ensure that functions assumed to malfunction independently in the safety analysis are not affected by failure of a single PDD in the platform. An HFC-FPGA platform-based safety system can also be configured to ensure that a single PDD malfunction or software error does not cause a spurious actuation of a safety function that is not enveloped in the plant design bases, accident analyses, anticipated transient without scram (ATWS) provisions, or other provisions for abnormal conditions.

Distribution of functions within an HFC-FPGA platform-based safety system is determined during application system development activities. The NRC staff considers an HFC-FPGA subsystem including an FPGA based module to be a single PDD for the purposes of the criteria of IEEE Std. 7-4.3.2-2003. As such, allocation of safety functions to a single HFC-FPGA subsystem should consider plant design bases, accident analyses, and ATWS provisions. This criterion is plant-specific and must be addressed during safety system development. See PSAI 5.2.16.

Completion of Protective Action:
The HFC-FPGA platform can be used to satisfy completion of protective action requirements. Once initiated, the RPS and ESF safety function actuations can be configured to proceed to completion. However, determination of IEEE Std. 603, Clause 5.2 compliance is a plant-specific evaluation item. See PSAI 5.2.15.

Quality:
The HFC-FPGA product line was designed for use in safety-related systems in NPPs. The design process used for the HFC-FPGA platform was therefore governed by HFC's QA program. The platform is maintained under a QA program intended to satisfy the requirements of Appendix B in all aspects of the product lifecycle, including design control, purchasing, fabricating, handling, shipping, storing, building, inspecting, testing, operating, maintaining, repairing, and modifying of the platform.

The HFC quality program is an updated version of the quality program that was used for the development of the HFC-6000 platform. As stated in the TR, the HFC QA program is designed to comply with NQA-1b-2011 Addenda to ASME NQA-1-2008, NQA-1-2012, and NQA-1-2015, "Quality Assurance Requirements for Nuclear Facility Applications," including the exceptions and clarifications identified in USNRC RG 1.28 Revision 5, Section C.

The TR states that following these industrial standards and regulatory guidance provides a basis for HFC Quality Assurance Program compliance with 10 CFR 50 Appendix B and 10 CFR Part 21. The TR also states that the HFC QA program complies with ISO 9001.

The HFC QAPM is organized such that Sections 1 to 18 correspond directly with Sections 1 to 18 of 10 CFR Part 50 Appendix B. Each section of the QAPM lists associated Quality Process Procedure (QPP) documents within the HFC quality program that provide details methods and instructions on how to carry out quality-related activities. The HFC QA program is implemented through QPPs, quality plans, process control sheets and work instructions.

HFC has been audited by an international utility member of the Nuclear Utility Procurement Issues Committee. To assure that the HFC QA program adheres to the QA programs, periodic third party, independent verification assessments are conducted to assure compliance with the QA program. This verification provides ongoing assessment of the adequacy of the measures undertaken to ensure technical correctness of the QA processes. HFC is a qualified supplier of Class 1E nuclear safety systems.

Based on the review of the HFC-FPGA platform application development processes, operating experience, lifecycle design output documentation, and testing and review activities, the NRC staff finds HFC-FPGA platform components and HFC QA processes to be acceptable for demonstrating built-in quality. Thus, the HFC-FPGA platform hardware and application logic implementations show adequate quality to be suitable for use in safety-related nuclear applications. Assuring supplier quality during application development is the responsibility of

the licensee. Thus, a licensee must assure that supplier quality is in accordance with the licensee's 10 CFR Part 50, Appendix B program. See PSAI 5.2.3.

The NRC staff determined the development processes used for the HFC-FPGA platform include development activities for system hardware, software and FPGA logic. The process also includes activities to facilitate the integration of the hardware, software and FPGA logic, and the integration of the HFC-FPGA modules with the safety system.

All HFC-FPGA platform hardware and software development and maintenance activities are governed by the QAPM as described in Section 6.8 of the HFC-FPGA platform TR. An evaluation of QA planning is provided in Section 3.3.1.3 of this SE.

Activities for development of HFC-FPGA platform-based I&C systems for US NPPs will be performed under the HFC QAPM. However, evaluation of development process implementation including system integration activities used for plant application software must be evaluated for compliance with Clause 5.3 of IEEE 7-4.3.2-2003 during plant application development. See PSAI 5.2.16.

Software Quality Metrics:
The responsibilities for the QA manager that are identified in QPP 1.2 include developing measurable data relating to the effectiveness of the HFC software QA program.

Software Tools:
Software tools used to support HFC-FPGA logic development activities are described in Section 7.0 of the HFC-FPGA platform TR. Several commercial tools are used to produce FPGA logic for the HFC-FPGA modules. The HFC-FPGA platform TR identifies the use of two different software tool methods during HFC-FPGA logic development.

A development tool called One-Step was developed by HFC to automate the process of converting a logic drawing into an HDL logic file and a programming file to be uploaded onto the FPGA device. The primary function of the One-Step software tool is to automate the logic translations. The tool is also capable of performing system on-line diagnostics by creating a dynamic indication of a Computer Aided Design drawing for display on a workstation so that logic drawings can be dynamically monitored with the system during operation.

The One Step tool was developed using a method that includes V&V of the tool to the same rigor as the highest software integrity level of the software being developed by the tool. Once an FPGA device is programmed with application logic, the FPGA based control system is then verified and validated via system testing. Therefore, the tool outputs which consist of the programmed FPGA modules are verified and validated independently from the tool that is used to develop the system. The NRC staff determined this method is consistent with both Methods a) and b) in IEEE Std. 7-4.3.2-2003 and is therefore acceptable.

Other third-party software tools used for HFC-FPGA logic development are not themselves developed to the same standards as the logic that performs safety functions. These tools have been verified through historical usage and their products are required by HFC V&V processes to be subject to testing to assure that any failure introduced by a tool will be detected. These tools are classified as non-safety related and are used in a manner such that defects not detected by the software tools will be detected by independent V&V activities described in the HFC V&V Plan and are corrected through the HFC corrective action programs. The NRC staff determined this method is consistent with Method b) of IEEE Std. 7-4.3.2-2003 and is therefore acceptable.

The NRC staff reviewed Section 7 of the HFC-FPGA platform TR and confirmed these tools are used in a manner, which is consistent with the criteria of IEEE Std. 7-4.3.2-2003 Clause 5.3.2. The NRC staff also confirmed that software tools used for HFC-FPGA logic development are controlled under the HFC configuration management program. The NRC staff could not evaluate the use of software tools for plant application logic development in this SE because no safety application was provided. The use and control of development tools for plant specific logic designs must be addressed during safety system application development. See PSAIs 5.2.2 and 5.2.16.

Verification and Validation:
The NRC evaluated the HFC Verification and Validation program, described in Sections 5.4 and 5.5 of the HFC-FPGA platform TR, and determined it to be compliant with the criteria of IEEE Std. 1012-2004, which is endorsed by RG 1.168. Though software is not used in the operating HFC-FPGA system, platform and application logic are developed using an integrity level that is equivalent to SIL 4, as defined in IEEE 1012-2004. Details of this evaluation are provided in Section 3.3.1.6 of this SE.

The NRC staff's evaluation of the verification and validation processes included an assessment of the type and level of independence maintained between the HFC V&V and product development organizations. The NRC staff determined the V&V organization is sufficiently independent from the organization performing design development activities.

Software Configuration Management:
The NRC evaluated the HFC configuration management program, described in Section 5.8 of the HFC-FPGA platform TR, and determined it to be compliant with the criteria of IEEE Std. 828-2005 as endorsed by RG 1.169. Details of this evaluation are provided in Section 3.3.1.7 of this SE. The NRC staff also confirmed that HFC configuration management program includes all the minimum required activities listed in Clause 5.3.5 of IEEE Std. 7-4.3.2-2003.

Software Project Risk Management:
Management planning for HFC-FPGA platform development activities include project oversight, control, reporting, review, and assessment of HFC-FPGA platform component design. The HFC management planning process is evaluated in Section 3.3.1.1 of this SE.

Equipment Qualification:
The HFC-FPGA platform is environmentally and seismically qualified to ensure the system is capable of performing its designated functions while exposed to normal, abnormal, test, accident and post-accident environmental conditions. Section 0 of this SE includes a detailed evaluation of HFC-FPGA EQ. However, licensee actions must be performed to address unique environmental conditions associated with a plant and to ensure that plant environmental conditions do not exceed the environmental limits to which the HFC-FPGA platform has been qualified. See PSAIs 5.2.5 through 5.2.8.

Computer System Testing:
Section 3.4 of this SE discusses the evaluation of the EQ program for the HFC-FPGA platform. HFC complied with the guidance of EPRI TR-107330 for the generic qualification of a PLC platform. EQ testing of the HFC-FPGA platform based representative system was performed while the test system modules were functioning. Test application logic and standard platform diagnostic functions, as described in Section 3.5.3 of this SE, representative of those to be used in actual operation were in operation during EQ testing.

The test application logic was specifically designed to support qualification testing of the HFC-FPGA platform while providing generic functionality of the test system. Based on the evaluation in Section 3.4 of this SE and review of the HFC-FPGA EQ summary test report (Reference 9), the NRC staff concludes that the qualification program met the requirement for computer testing of the HFC-FPGA platform, subject to satisfactory resolution of plant specific action items (PSAIs) in Section 5.2 of this SE.

Qualification of Existing Commercial Computers:
HFC-FPGA platform components are designed and developed by HFC under the HFC quality assurance program. Therefore, the platform modules do not require commercial grade dedication. There are components of the platform however, such as library modules and IP cores, that are developed commercially and thus require commercial grade dedication by HFC. Such dedication activities are performed in accordance with EPRI TR-106439 and EPRI TR-107330 under the HFC QA program.

System Integrity:
Determination of system integrity is a plant-specific activity that requires an assessment of a full system design against a plant specific design basis. A platform-level assessment can only address those characteristics that support fulfillment of this requirement by a system design based on the platform. Since the HFC-FPGA platform TR does not address a specific application or establish a definitive safety system design, the evaluation against this requirement is limited to consideration of the integrity demonstrated by the HFC-FPGA platform and its features to assure a safe state can be achieved in the presence of failures. While the evaluation indicates the suitability of the platform to contribute to satisfying this requirement, a plant-specific evaluation is necessary to establish full conformance with Clause 5.5 of IEEE Std. 603-1991.

The HFC-FPGA platform design has several characteristics that can be used to establish a high level of system integrity. These characteristics are described and evaluated in Section 3.5 of this SE. HFC-FPGA platform components are qualified to ranges of conditions that are typically acceptable for NPP applications. Licensees using an HFC-FPGA based safety system are required to ensure that enumerated plant design conditions are within the conditions for which the HFC-FPGA platform components are qualified.

HFC-FPGA based systems are designed to operate in a deterministic manner. The NRC staff evaluated the deterministic attributes of the HFC-FPGA platform and the results of that evaluation are in Section 3.5.2 of this SE. Deterministic performance and high reliability are attributes of the HFC-FPGA platform, which can support compliance with System Integrity criteria of Clause 5.5 of IEEE Std. 603-1991.

Design for Computer Integrity:
The HFC-FPGA platform includes features to provide fault detection and mitigation capabilities. The HFC-FPGA platform includes diagnostics and self-testing (see Section 3.5.3 of this SE) that support a high level of system integrity. HFC-FPGA platform integrity is evaluated in Section 3.5 of this SE. However, HFC did not define a specific system architecture or application for the platform. Instead, HFC defined a generic platform that can be used in a wide range of applications or configurations. Therefore, the NRC staff only evaluated the features provided in the generic platform. This evaluation can be used to support development of future plant-specific logic applications.

The HFC-FPGA platform qualification activities discussed in Section 3.4 of this SE, provide suitable evidence that the platform can maintain plant safety when subjected to environmental conditions that have the potential to defeat implemented safety functions.

The NRC staff determined that fault detection and mitigation design features provided for the HFC-FPGA platform can be used to facilitate performance of safety functions in a reliable manner. Determination of compliance with the criterion of IEEE Std. 7-4.3.2-2003 Clause 5.5.1 requires a plant-specific action item to address system integrity for a plant-specific application (see Sections 5.2.13 and 5.2.16).

Design for Test and Calibration:
Online self-diagnosis and test functions are provided in the HFC-FPGA platform to support test and calibration requirements. These are described in Section 6.3 of the HFC-FPGA platform TR and are evaluated in Section 3.5.3 of this SE.

Qualification tests performed for the HFC-FPGA platform were conducted with self-diagnosis functions operating in conjunction with the test application performing basic functions. See HFC-FPGA Equipment Qualification Summary Test Report (Reference 9) for additional information on these tests. The performance of the HFC-FPGA equipment during these tests demonstrated that diagnosis features did not adversely affect the ability of the system to perform its functions. Therefore, the NRC staff determined the diagnosis capabilities provided by the HFC-FPGA platform conform to this requirement.

Maintenance activities performed on an HFC-FPGA based safety system, including periodic surveillance testing, will be defined based on the plant-specific system requirements. Determination of test and calibration requirements and establishment of surveillance tests necessary to ensure that the identifiable single failures are detected are plant-specific activities. See PSAI 5.2.12.

Fault Detection and Self-Diagnostics:
Section 3.5.3 of this SE provides an evaluation of the HFC-FPGA platform diagnostics and self-test capabilities. These tests and diagnostics provide functions to detect failures in the system hardware, as well as to detect system failure modes identified in the HFC-FPGA FMEA (Reference 10). See Section 3.3.2.5 of this SE for more information on the HFC-FPGA FMEA.

If errors are encountered during system operation, self-diagnosis features will respond by either providing an alarm or by setting output signals to pre-defined states depending on the severity of the fault identified. Alarms or predefined states are to be defined during plant system development and plant-specific failure analysis should be performed for each plant-specific application.

Hardware and software based diagnostic features of the HFC-FPGA platform provide an acceptable method of detecting and reporting system faults and failures in a timely manner. The HFC-FPGA platform is therefore acceptable for providing fault detection in support of safety-related applications. However, because HFC did not define the actions to be taken when faults are detected, and did not identify specific self-tests or periodic surveillance testing necessary to detect and address the effects of system failures on plant safety, there may be additional fault-detection and diagnostic function requirements to provide more comprehensive coverage of identified system failures. Therefore, determination of IEEE Std. 7-4.3.2-2003, Clause 5.5.3 compliance is a plant-specific evaluation item. See PSAIs 5.2.12 and 5.2.16.

Independence:
The redundancy characteristics of an HFC-FPGA platform-based safety system are defined at the system level during the application development. Therefore, the determination of independence is a plant-specific activity that requires an assessment of a full system design. See PSAIs 5.2.14 and 5.2.16.

A platform-level assessment can only address those characteristics of the platform that can support fulfillment of this requirement by a system design based on the platform. The platform's evaluation against this requirement is limited to consideration of the digital communications for the system, which are described in Section 3.2.3 and evaluated in Section 3.8 this SE.

Independence Between Redundant Portions of a Safety System:
The HFC-FPGA platform does not include design provisions to support communications between different safety divisions. Therefore, this criterion does not apply to an HFC-FPGA platform-based system.

Independence Between Safety Systems and Effects of Design Basis Event:
Determining the effects of design basis events and establishing the physical separation of the safety system from the effects of those events are plant-specific activities. However, the qualification of the HFC-FPGA platform can be used to demonstrate the capability of a safety system based on the platform to satisfy this requirement. The evaluation of the EQ for the HFC-FPGA platform is contained in Section 3.4 of this SE. This SE identifies plant-specific actions to demonstrate that the platform performance as bounded by its EQ satisfies the requirements of the plant-specific installation environment for the plant-specific safety functions. See PSAIs 5.2.5 through 5.2.8.

Independence Between Safety Systems and Other Systems:
The HFC-FPGA platform provides digital communication design features that can support independence between a platform-based safety system and other interfacing systems. These platform design features are described in Section 3.2.3 and evaluated in Section 3.8 of this SE.

Communication from an HFC-FPGA based safety system to an external system can be performed using one-way C-Link communications interfaces through FPC08 gateway modules. The NRC staff determined that one-way C-Link communications can be used to provide an acceptable means of performing communications to external systems.
Though compliance with this clause remains a plant-specific requirement, these design characteristics of the HFC-FPGA platform can be used in a plant specific design to support conformance to the criteria of Clause 5.6.3 of IEEE 603 1991.

The NRC staff finds that the communications capabilities of the HFC-FPGA platform provide acceptable design features to enable communications independence when appropriately configured. However, the specific interconnections defined for an application must be determined and addressed during plant application development. See PSAI 5.2.14 of this SE for plant specific action items.

Compatibility for Testing and Calibration:
The diagnostic functions described in Section 3.5.3 of this SE can be used to support compliance with system test and calibration requirements. However, determination of full compliance with these criteria is dependent on the specific safety system design as well as the plant specific safety functions performed by the system. Therefore, determination of IEEE 603, Clause 5.7 compliance is a plant-specific evaluation item. See PSAI 5.2.15.

The NRC staff evaluated the HFC-FPGA self-diagnosis and test and calibration capabilities for compliance with the criteria of IEEE 7-4.3.2-2003 Clause 5.7. The platform design includes self-diagnostics features to detect failures within the HFC-FPGA based safety system during operation. The use of Wireless receivers/transmitters on temporarily connected measurement and test equipment is not discussed in the HFC-FPGA platform TR and is therefore not applicable to the platform. There are also no requirements or expectations that HFC-FPGA configuration changes would need to be made to support periodic automated or manual surveillance testing.

The level of complexity introduced to the HFC-FPGA platform by the diagnostic features described in Section 6.3 of the HFC-FPGA platform TR was determined to be commensurate with the safety functions to be performed and the benefits provided by these features justify their inclusion into the platform design. The NRC staff finds that the HFC-FPGA platform complies with the criteria of IEEE Std. 7-4.3.2-2003 Clause 5.7. However, a plant specific activity to analyze diagnostic functions to be included in plant application logic should also be performed. See PSAI 5.2.16.

Control of Access:
The platform design includes provisions for controlling access to HFC-FPGA equipment while in service. These provisions include physical access controls to modules, logic access controls and software access controls. Use of these provisions can be administratively controlled by the system operators. Implementation of administrative controls is a plant application specific activity which must be performed during plant application development. See PSAI 5.2.15.

Repair:
The HFC-FPGA platform is designed with self-diagnostic features that support timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment. These features can be used to support compliance with this criterion. Section 3.5.3 of this SE includes an evaluation of platform self-diagnostic features. The NRC staff determined the HFC-FPGA platform design is generally capable of supporting the criteria of Clause 5.10; however, some aspects of a system repair capabilities must be determined during application development and therefore compliance with this position should be confirmed during plant application development. See PSAI 5.2.15.

Reliability:
A reliability analysis was performed for the HFC-FPGA platform modules. The NRC staff evaluation of HFC-FPGA platform reliability is provided in Section 3.3.2.6 of this SE. The NRC staff determined the HFC-FPGA platform TR contains platform reliability information that can be used to demonstrate conformance to plant specific reliability goals. Because reliability goals are established on a plant specific basis, a determination of whether plant and system specific goals are met must be made at the time of application development. See PSAIs 5.2.10 and 5.2.13.

Identification:
Establishing software/firmware identification requirements and providing the means for retrieving that identification information are directly related to the HFC configuration management program. Section 3.3.1.7 of this SE contains the evaluation of the HFC configuration management process as it applies to maintaining the configuration of HFC-FPGA platform logic.

Identification requirements specific to HFC-FPGA platform logic are used to assure the correct platform logic and logic library modules are installed into the correct system modules. Identification of installed logic can be performed using an HFC engineering workstation. Physical identification of the HFC hardware modules will be performed in accordance with the identification requirements in IEEE Std. 603-1991 Clause 5.11.

Based on the processes reviewed and observed during the regulatory audit for HFC-FPGA logic identification, the NRC staff determined the HFC-FPGA platform complies with the guidance of IEEE Std. 7-4.3.2-2003 Clause 5.11 for its platform logic. However, assurance that proper hardware and plant application logic configuration is established and maintained is an activity that must be performed during plant application development and implementation. See PSAI 5.2.16.

3.9.3 Sense and Command Features – Functional and Design Requirements

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

Specifically, the following requirements were not evaluated:

- Clause 6.1, Automatic Control
- Clause 6.2, Manual Control
- Clause 6.3, Interaction between Sense and Command Features and other Systems
- Clause 6.4, Deviation of System Inputs
- Clause 6.6, Operating Bypass
- Clause 6.7, Maintenance Bypass.

Capability for Testing and Calibration:
The HFC-FPGA platform design includes features that permit testing during power operation. The HFC-FPGA platform design does not require disconnecting wires, installing jumpers, or other similar modifications of installed equipment to accomplish required system testing to verify operability of the safety system. The NRC staff review of the HFC-FPGA platform self-diagnostics, test and calibration capabilities is provided in Section 3.5.3 of this SE. Because determination of specific input sense and command requirements are plant-specific, the NRC staff considers this criterion to be a plant specific action. See PSAI 5.2.15.

Setpoints:
This requirement for setpoints primarily addresses factors beyond the scope of a digital platform (e.g., plant design basis limits, modes of operation, and sensor accuracy). The HFC-FPGA platform TR does not address a specific application or establish a definitive safety system, which is necessary to demonstrate the adequacy of setpoints that are associated with IEEE Std. 603-1991 Clause 4.4. The NRC staff's review of HFCs approach to setpoint determination is provided in Section 3.6 of this SE. Because determination of setpoints is not performed at the generic platform level, compliance with this criterion to determine adequacy of established setpoints remains a plant-specific activity, which must be performed during system development. See PSAI 5.2.11.

3.9.4 Execute features – functional and design requirements

Since the HFC-FPGA platform TR does not address a specific application of the platform, include the sensors, nor provide a specific safety system design, the functional and design requirements for a safety system are not available for review and no evaluation of the HFC-FPGA platform against these regulatory requirements could be performed. Specifically, the following IEEE Std. 603-1991 requirements were not evaluated:

- Clause 7.1, “Automatic Control”
- Clause 7.2, “Manual Control”
- Clause 7.3, “Completion of Protective Action”
- Clause 7.4, “Operating Bypass”
- Clause 7.5, “Maintenance Bypass.”

Establishment of compliance with these criteria is a plant specific action. See PSAI 5.2.15.

3.9.5 Power Source Requirements

Power supply requirements for the HFC-FPGA platform are described in Section 5.1.3, “Power Distribution and Chassis,” of the platform TR. An HFC-FPGA system typically receives power from two redundant 24 VDC power sources. These power inputs are distributed to each of the system modules through connections on the chassis backplane. The platform also includes provisions for use of an isolated auxiliary power supply that can be used to provide excitation power for external sensors. The power supply modules and racks used in the HFC-FPGA platform are the same as those used in the HFC-6000 platform. The use of power sources external to the HFC equipment is a plant-specific activity and will need to be addressed during plant system development. See PSAI 5.2.15.

3.10 Secure Development and Operational Environment

Regulatory positions 2.1 – 2.5 of RG 1.152, Revision 3 identify controls that an applicant should implement during the development activities for safety-related digital systems. The HFC-FPGA platform is specifically developed for nuclear applications and it includes security features that can be used to prevent or mitigate the effects of inadvertent access during development and operation.

Section 6.11.2, “Secure Development and Operational Environment Controls” of the HFC-FPGA platform TR describes the platform development environment, platform vulnerability assessment, and the implementation of Secure Development and Operational Environment (SDOE) controls. This section states the following:

> Security controls for a safety-related system development and operational environment were developed after a risk assessment of the HFC-FPGA system. This includes the identification of critical digital assets, development of defensive safeguards for these critical digital assets, and testing to ensure the safeguards in place are functioning as required.

The NRC staff evaluated the HFC-FPGA SDOE to confirm compliance with the criterion of RG 1.152 as follows. For criteria that could not be evaluated, PSAI 5.2.17 specifies actions to be performed during plant specific application development.

3.10.1 Concepts Phase

Identification and Description of Secure Operational Environment Design Features:
HFC has implemented security controls for the HFC-FPGA platform that are intended to eliminate vulnerabilities associated with the digital equipment development processes. Some examples of security controls are listed in Section 6.11.2 of the HFC-FPGA platform TR.

Assessment of Potential Susceptibilities:
HFC addressed this part of the regulatory position by performing vulnerability assessments. Section 6.11.1, "Vulnerability Assessment" of the TR describes the vulnerability assessment process. In this process, the HFC V&V team conducts security analysis at various lifecycle phases and documents the security vulnerabilities identified during each development phase. Control measures are then used to address those identified vulnerabilities.

Platform vulnerabilities in the development lifecycle phases of the HFC-FPGA modules were determined to be comparable to those identified for the HFC-6000 platform. A summary of these vulnerabilities by phases is provided in Section 6.11.1 of the HFC-FPGA platform TR.

This analysis identifies the platform development assets, vulnerabilities and secure controls used to identify and mitigate risks associated with unwanted, unneeded and undocumented functionality being introduced during system development or modification activities. This HFC development environment vulnerability assessment includes assessments of hardware, software and logic, configuration, and network vulnerabilities. The NRC staff finds these vulnerability assessment activities can be used to show compliance with the criteria of RG 1.152 Position 2.1; however, the establishment of a secure environment for application logic development remains a plant specific action. See PSAI 5.2.17.

Remote Access:
Evaluation of a safety system against this part of the regulatory position is a plant-specific activity that requires an assessment of a completed system design. The HFC-FPGA platform design partially addresses this part of the regulatory position by incorporating design features that limit connectivity between HFC-FPGA safety systems and other external systems. Section 3.2.3 of this SE describes external communications interfaces of the HFC-FPGA platform and Section 3.8 of the SE evaluates these interfaces for regulatory compliance. These interfaces include features that can be credited to restrict remote accessibility for HFC-FPGA based systems. See PSAI 5.2.17.

3.10.2 Requirements Phase

Definition of Secure Operational Environment Functional Requirements:
The compliance of a safety system with this part of the regulatory position was not evaluated because defining and establishing requirements for external C-Link communication interfaces is a plant-specific activity that requires an assessment of the plant specific safety system design. See PSAI 5.2.17.

Verification of SDOE Requirements:
Section 6.11.2 of the HFC-FPGA platform TR identifies SDOE controls that are included in the platform design. The identified controls include: version management, password protection, physical access control, and checksum verification. These SDOE features have been implemented in accordance with the platform development processes described and evaluated in Section 3.3 of this SE.

These development processes provide a framework for establishing correctness, completeness, accuracy, testability, and consistency attributes and were determined by the NRC staff to be acceptable. Plant application specific SDOE features may also be identified during system requirements development activities. Such features would need to be included as application design requirements and would need to be incorporated into the application logic during the application development process. See PSAIs 5.2.2 & 5.2.17.

Use of Predeveloped Software (Logic) and Systems:
The HFC-FPGA platform modules and FPGA logic designs are developed and maintained in accordance with HFCs quality assurance program. Section 3.3.1.3 of this SE includes an NRC assessment of the HFC QAPM processes.

Certain elements of the HFC-FPGA platform logic are pre-developed and are subject to plant application specific safety system reliability requirements. See Sections 3.3.2.6, “Reliability Analysis” and 3.2.4, “IP Cores” of this SE for additional information and required actions pertaining to the use of pre-developed FPGA logic. Application FPGA logic will be developed by HFC under its QA programs and in accordance with a licensee’s 10 CFR 50, Appendix B QA processes. See PSAI 5.2.2 for more information on vendor oversight activities to be performed during application development. The NRC staff finds that HFC development processes can be used show compliance with the criteria of RG 1.152 Position 2.2; however, reliability requirements are plant specific and therefore must be verified during application logic development. See PSAI 5.2.17.

Prevention of the Introduction of Unnecessary Requirements:
Evaluation of a safety system against this part of the regulatory position is a plant-specific activity that requires an assessment of a completed system design. See PSAI 5.2.2 for more information on V&V activities to be performed during application development including the development of system requirements specifications. HFC partially addresses this part of the regulatory position by requiring an independent reviewer check the requirements specifications in order to detect and correct the insertion of requirements that have an undesirable effect on the secure operational environment of the system. This ensures that the secure operational environment features of the HFC-FPGA platform are not compromised by changes or the introduction of new functions or products to the platform design. The NRC staff finds that secure operational environment features can be used show compliance with the criteria of RG 1.152, Position 2.2; however, the additional plant specific actions must be taken to ensure that unnecessary requirements are not included in the application logic. See PSAI 5.2.17.

3.10.3 Design Phase

System Features: Translation of SOE Requirements into Design Configuration Items:
Evaluation of a safety system against this part of the regulatory position is a plant-specific activity that requires an assessment of a completed system design. See PSAI 5.2.2 for more information on V&V oversight activities to be performed during application development including development of a system design description. HFC partially addresses this part of the

regulatory position by using requirements traceability methods to confirm the traceability of the HFC-FPGA platform SDOE features from requirements to design specifications. See Section 3.3.2.3 of this SE for evaluation of the HFC requirements traceability processes. See PSAI 5.2.17.

Physical and Logical Access Controls:
HFC partially addresses this part of the regulatory position because the physical, logical and administrative access control features established for platform logic development are based on the results of the completed vulnerability analysis. Evaluation of a specific safety system against this part of the regulatory position is a plant-specific activity that requires an assessment of a completed system design. See PSAI 5.2.2 for more information on V&V oversight activities to be performed during application development including performance of an application development environment vulnerability assessment.

During its regulatory audit, the NRC staff reviewed the platform vulnerability analysis report and determined that vulnerability assessments are used show compliance with the criteria of RG 1.152, Position 2.3 for platform logic physical and logical access control functions. The results of the NRC regulatory audit are documented in Reference 13. The implementation of physical and logical access controls into application logic remains a plant specific action. See PSAI 5.2.17.

The HFC-FPGA platform secure development environment ensures that no unintended logic is included in the platform and related documentation during platform logic development, and that unintended changes to the platform logic installed in the system are prevented.

HFC implements configuration control measures to: detect unauthorized changes to controlled documents (e.g., specifications, design descriptions and test reports); control access to the document control system and the logic design development and storage environment; independently verify that the content of production copies of logic designs match the controlled master copies, label controlled media and storage devices, and identify logic design versions that are under development, approved for production, and retired.

The HFC-FPGA platform security measures that are designed to eliminate credible vulnerabilities associated with security management and the digital equipment development process have been implemented. However, the review of the application logic secure development environment controls implemented in an HFC-FPGA platform-based system is a plant-specific activity. See PSAI 5.2.17 for further information on this activity.

The programming ports used to modify HFC-FPGA logic on system modules are inaccessible during normal system operation. To modify system platform or application logic designs, the associated module must be removed from the operational chassis and placed into an extender board, which allows access to the programming ports on the module circuit board. Removal of a module generates a signal that can be used to initiate an alarm in the main control room. The NRC staff finds that the HFC-FPGA platform contains secure operational environment features that can be used to support the plant specific safety applications. Because determination of a secure operational environment is a plant specific activity, the NRC staff considers this criterion to be a plant specific action. See PSAI 5.2.17.

Prevention of the Introduction of Unnecessary Design Features:
HFC development processes partially address this part of the regulatory position by requiring an independent review of the FPGA logic design specifications in order to detect and correct the

insertion of design features that could have an undesirable effect on the secure operational environment of the system. Requirements traceability methods are used to verify that the secure operational environment features from the requirement phase are correctly translated into the design, and to ensure that unauthorized functionality is not introduced into the design. The NRC staff finds that HFC processes for verifying the translation of SDOE design features is acceptable and can be used to support the plant specific application of the HFC-FPGA platform. Because determination of a secure operational environment is a plant specific activity, the NRC staff considers this criterion to be a plant specific action. See PSAI 5.2.17.

3.10.4 Implementation Phase

Transformation from System Design Specification to Design Configuration Items:
HFC development processes partially address this part of the regulatory position by using requirements traceability methods. Requirements traceability methods are used to verify that the secure operational environment features from design specification to design configuration items.

The NRC staff determined that HFC processes for verifying the translation of SDOE design specifications is acceptable and can be used to support the plant specific application of the HFC-FPGA platform. Because determination of a secure operational environment is a plant specific activity, the NRC staff considers this criterion to be a plant specific action. See PSAI 5.2.17.

Implementation of Secure Development Environment Procedures and Standards:
HFC addresses this part of the regulatory position through implementation of development environment control procedures and by implementing physical, logical and administrative controls to construct and maintain a secure development environment that minimizes the potential for unintended modifications to the system.

During the regulatory audit, the NRC staff reviewed HFC procedures used to implement the secure development environment and found them to be adequate means of establishing and maintaining the secure platform development environment. The NRC staff finds that HFC secure platform development environment controls and procedures meet the criterion of regulatory position 2.4 and are therefore acceptable. Establishment of a secure development environment for application logic development remains a plant specific activity which must be performed during application logic development. See PSAI 5.2.17.

Accounting for Hidden Functions in the Code:
HFC addresses this part of the regulatory position by performing various V&V activities. An independent V&V team is used to check the system FPGA logic designs and logic library modules. The independent V&V team verifies the logic designs by performing functional and structural unit testing, which would detect and correct the insertion of functions and vulnerable features that would have an undesirable effect on the secure operational environment of the system. The NRC staff evaluated the V&V processes and activities used for HFC-FPGA platform development. See Sections 3.3.1.6 and 3.3.2.2 of this SE for more information on this evaluation.

The NRC staff finds that HFC processes for detecting and addressing errors in the platform and FPGA logic implementation are acceptable and can be used to support the plant specific application of the HFC-FPGA platform. Because determination of a secure operational

environment is a plant specific activity, the NRC staff considers this criterion to be a plant specific action. See PSAI 5.2.17.

3.10.5 Test Phase

Validation of *Secure Operational Environment Design Configuration Items:*
The compliance of a safety system with this part of the regulatory position was not evaluated because it is an activity that requires an assessment of the plant-specific safety system design. See PSAI 5.2.17.

Configuration of Secure Operational Environment Design Features:
The compliance of a safety system with this part of the regulatory position was not evaluated because it is an activity that requires an assessment of the plant-specific safety system design. See PSAI 5.2.17.

4.0 SUMMARY

The NRC staff determined the HFC-FPGA platform, consisting of modules described in the HFC-FPGA platform TR, their design features, the platform logic embedded in electronic boards and the processes used to produce them are sufficient to support compliance with the applicable regulatory requirements for a plant-specific use for safety-related I&C systems. This determination is applicable for use of the HFC-FPGA platform in safety-related applications provided that each plant-specific use satisfies the limitations and conditions delineated in Section 5.0 of this SE and the system is properly installed and used. The NRC staff further concludes that the HFC-FPGA platform can be used in safety-related systems to provide reasonable assurance of adequate protection of public health, safety and security based on the technical evaluation provided in Section 3.0 of this SE. On this basis, the NRC staff determined the HFC-FPGA platform is acceptable for use in safety-related Instrumentation and Control systems.

5.0 LIMITATIONS AND CONDITIONS

The items within this section provide limitations and conditions for use of the HFC-FPGA platform. For each applicable GOI and plant-specific action item, an applicant or licensee referencing this SE should demonstrate that applicable items have been satisfactorily addressed.

5.1 Generic Open Items

The following GOI must be resolved to establish acceptability of the platform for general use in implementing safety-related applications at nuclear power plants.

5.1.1 Restrictions on FCPU I/O Functionality – The eight digital output channels and eight digital input channels in the HFC-FCPU are not approved for use in safety related applications of the HFC-FPGA platform. An applicant or licensee referencing this SE for

a safety-related plant-specific application should therefore ensure these digital input and output interfaces are excluded from any safety system design.

5.2 Plant Specific Action Items

The following plant-specific actions should be performed by an applicant or licensee referencing the HFC-FPGA platform TR for a safety-related system based on the HFC-FPGA platform.

5.2.1 HFC-FPGA Platform Changes – An applicant or licensee referencing the HFC-FPGA platform TR should demonstrate that the HFC-FPGA platform used to implement the plant-specific system is unchanged from the generic platform addressed in this SE. Otherwise, the licensee should identify any modification or addition to the generic HFC-FPGA platform as it is employed and provide evidence of compliance by the modified platform with all applicable regulations that are affected by the changes. In addition, the applicant must verify that modules, features, and or functions that require configuration are properly configured and tested to meet system requirements.

5.2.2 Application Logic Development Process – An applicant or licensee referencing the HFC-FPGA platform TR should provide oversight to ensure the development of its Application Logic is performed in accordance with an acceptable development process that is equivalent to the processes described in Sections 5.4, FPGA Software Development Process" and 5.5, "FPGA Specific Implementation" of the HFC-FPGA platform TR and evaluated in Section 3.3 of this SE.

5.2.3 Quality Assurance - An applicant or licensee must demonstrate that execution of the HFC software QA program, with its constituent lifecycle processes, plans, and procedures, for the planning, design, implementation, testing, and installation of application software, along with the introduction of any new functionality within the operating software (i.e., new software), complies with the regulatory requirements of Appendix B to 10 CFR Part 50 and is equivalent to industry standards and practices endorsed by the NRC, as referenced in SRP BTP 7-14 (see Sections 3.3.1.1 and 3.3.1.3 of this SE).

5.2.4 System response time –The capability of the HFC-FPGA platform to satisfy application-specific requirements for system response time must be demonstrated on a plant-specific basis to assure compliance with accident analyses requirements of the safety system (see Section 3.5.1 of this SE).

5.2.5 Plant Specific Equipment Environmental Qualification – Licensees using the HFC-FPGA platform must ensure their plant-specific conditions and levels, such as environmental (temperature and humidity), seismic, ESD, electrical power surge, and EFT are enveloped by the corresponding qualification profiles used to qualify the HFC-FPGA platform modules evaluated in this SE. Otherwise, the HFC-FPGA based system must be demonstrated to be qualified for the plant specific environmental conditions.

5.2.6 Harsh Environment - Licensees using the HFC-FPGA platform in a non-mild environment must demonstrate that an HFC-FPGA based system is qualified for its use

in harsh environments as defined in 10 CFR 50.49, which includes temperature, pressure, humidity, radiation, chemicals, and submergence conditions.

5.2.7 Smoke - Because fire smoke may have adverse impact on the performance of the HFC-FPGA platform, licensees using the HFC-FPGA platform in a specific application must demonstrate that an HFC-FPGA based system is qualified for potential smoke exposures if smoke from any fire could become a hazard for the system.

5.2.8 Platform Module Version Qualification – Only the specific HFC-FPGA platform modules used in the QTS are qualified. Licensees referring to the HFC-FPGA platform must ensure that a different, similar HFC-FPGA module or even a same module with a different version needs to be qualified or justified before its use.

5.2.9 Failure Modes and Effects Analysis – An applicant or licensee referencing the HFC-FPGA platform TR must perform a system-level FMEA to demonstrate that the application-specific use of the HFC-FPGA platform identifies each potential failure mode and determines the effects of each. The HFC-FPGA FMEA (evaluated in Section 3.3.2.5 of this SE) is intended to be used as input data to support a system-level FMEA and reliability analysis for an NPP-specific HFC-FPGA platform system.

The FMEA should demonstrate that single failures, including those with the potential to cause a non-safety system action that results in a condition requiring protective action (i.e., a protection function), cannot adversely affect the protection functions, as applicable.
The applicant or licensee should ensure system failure states identified in the FMEA are consistent with system requirements and should determine how errors and failures are indicated and managed upon being detected.

5.2.10 Plant Application Specific System Reliability – An applicant or licensee referencing the HFC-FPGA platform TR should perform a system-level evaluation of the degree of redundancy, diversity, testability, and quality provided in a HFC-FPGA platform-based safety system to determine if the degrees provided are commensurate with the safety functions being performed. An applicant or licensee should ensure that a resultant HFC-FPGA platform-based system satisfies applicable reliability goals that the plant has established for the system.

This plant-specific action should consider the effect of possible failures, system-level design features provided to prevent or limit the failures' effects, and any application-specific inclusion of a maintenance bypass functionality to support plant operations.

5.2.11 Setpoint Methodology – An applicant or licensee referencing this SE must perform an analysis of accuracy, repeatability, thermal effects and other necessary data for use in determining the contribution of the HFC-FPGA platform to instrumentation uncertainty in support of setpoint calculations.

5.2.12 System Testing and Surveillance – Because a combination of surveillance, HFC-FPGA diagnostics and automatic self-tests are necessary to provide comprehensive coverage of platform failures, the applicant or licensee referencing this SE must establish periodic surveillance testing necessary to detect system failures for which automatic detection is not provided. The applicant or licensee must also define appropriate surveillance

intervals to provide acceptable comprehensive coverage of identifiable system failure modes.

5.2.13 Diversity and Defense-In-Depth (D3) Analysis – An applicant or licensee referencing this SE must perform a plant-specific D3 analysis for safety system applications of the HFC-FPGA platform.

5.2.13.1 Self-Diagnostics Design Requirements – The licensee must establish requirements for enabling and testing necessary self-diagnostics features used to identify and address postulated control or protection logic common cause failures within the HFC-FPGA safety system.

5.2.13.2 Plant Specific Fail-Safe Behavior Requirements Definition – Fail Safe state requirements shall be established by the applicant or licensee for all safety functions to ensure plant safety is achieved when HFC-FPGA system logic failures are detected by system self-diagnostic functions.

5.2.13.3 Conservation of Existing Diversity Measures – The applicant or licensee must ensure that diversity attributes of the existing protection system are preserved in the upgraded system. This diversity may be expressed in the signal selection and protection system functional algorithms established and accepted for the plant design.

5.2.14 Communications (DI&C ISG-04) – Although the NRC staff determined that the HFC-FPGA platform includes features to support satisfying various sections and clauses of DI&C-ISG-04, an applicant or licensee referencing this SE must evaluate the HFC-FPGA platform based-system for compliance with this guidance. The applicant or licensee should consider its plant-specific design basis. This SE does not address a specific application, establish a definitive safety system or protective action, or identify and analyze the impact of credible events along with its direct and indirect consequences.

5.2.15 IEEE Std. 603 – Although the NRC staff determined that the HFC-FPGA platform can satisfy various sections and clauses of IEEE Std. 603-1991, an applicant or licensee referencing the HFC-FPGA platform TR should identify the approach taken to satisfy each applicable clause of IEEE Std. 603-1991 with consideration of the plant-specific design basis.

This SE does not address a specific application, establish a definitive safety system or protective action, or identify and analyze the impact of credible events including direct and indirect consequences. Therefore, an applicant or licensee should ensure that the plant-specific and application-specific use of the HFC-FPGA platform satisfies the applicable IEEE Std. 603-1991 clauses in accordance with the plant-specific design basis and safety system application.

5.2.16 IEEE Std. 7-4.3.2-2003 – Even though the NRC staff determined that the HFC-FPGA platform is capable of satisfying various sections and clauses of IEEE Std. 7-4.3.2-2003, an applicant or licensee referencing this SE should identify the approach taken to satisfy each applicable clause of IEEE Std. 7-4.3.2-2003 with consideration of the plant-specific design basis.

This SE does not address a specific application, establish a definitive safety system or protective action, or identify and analyze the impact of credible events including direct

and indirect consequences. Therefore, the applicant or licensee should demonstrate that the plant-specific and application-specific use of the HFC-FPGA platform satisfies the applicable IEEE Std. 7-4.3.2-2003 clauses in accordance with the plant-specific design basis and safety system application.

5.2.17 Secure Development and Operational Environment – An applicant or licensee referencing this SE for a safety-related plant-specific application should ensure that a SDOE has been established for its plant-specific application, and that it satisfies the applicable regulatory evaluation criteria of RG 1.152."

5.2.18 Class 1E to Non-Class 1E Isolation - The applicant or licensee should ensure that all HFC-FPGA interfaces between Class 1E and Non-1E circuits do not exceed the maximum test voltages to which the HFC-FPGA equipment is qualified to operate. See Section 3.4.2 of this SE for boundary conditions established for the HFC-FPGA platform during the isolation capability testing.

6.0 REFERENCES

1. Submittal of Non-proprietary information for Amendment 4 to the HFC-6000 Safety Platform, April 15, 2019 (Agencywide Documents and Management System (ADAMS) Package Accession No. ML19109A165, letter ML19109A158).
2. HF Controls Corporation topical report, proprietary version, "Amendment for HFC-FPGA System of HFC-6000 Safety Platform," RR901-107-10, Revision F, April 3, 2019 (ADAMS Accession No. ML19109A157).
3. HF Controls Corporation topical report, non-proprietary version, "Amendment for HFC-FPGA System of HFC-6000 Safety Platform," RR901-107-10, Revision F, dated April 3, 2019 (ADAMS Accession No. ML19109A156).
4. HF Controls Corp. letter to NRC, "Doosan-HF Controls and Doosan Heavy Industries & Construction Submittal of Topical Report for Safety Evaluation," March 5, 2008 (ADAMS Accession No. ML080780169).
5. "Transmittal of NRC Approved Topical Report PP901-000-01CF-P/NP-A, HFC-6000 Safety Control System." Package includes NRC SE and approved TR. June 27, 2011 (ADAMS Package Accession No. ML111880583).
6. HF Controls Corp. letter to NRC, "Request for Amendment to HFC-6000 Safety Evaluation Report (TAC No. MD8462)," June 29, 2011 (ADAMS Accession No. ML11199A098)
7. "Final Safety Evaluation for the Closeout of Open Items Related to Doosan HF Control Corporation Topical Report PP901-000-01, Revision C, "HFC-6000 Safety System" (TAC ME7577)" March 4, 2015 (ADAMS Accession No. ML15061A181).
8. NRC letter to HF Controls Corp., "Acceptance Review and Requests for Withholding of "Submittal of Non-proprietary information for Amendment 4 to the HFC-6000 Safety Platform" (L-2018-TOP-0031), June 14, 2019 (ADAMS Accession No. ML19127A009).
9. HF Controls Corp. HFC-FPGA Equipment Qualification Summary Test Report," TR901-302-02, Revision B, May 19, 2020 (ADAMS Accession Nos. ML20195A836 Proprietary & ML20195A821 Non-Proprietary).
10. HF Controls Corp., "Failure Modes and Effects Analysis for the HFC-FPGA Platform Functions and System," RR-901-107-11-P, Revision A, February 5, 2020 (ADAMS Accession Nos. ML20071F396 Proprietary & ML20071F335 Non-Proprietary).
11. NRC Request for Additional Information for Amendment 4 to the HFC 6000 Safety Platform, February 19, 2020 (ADAMS Accession Nos. ML20021A232 Proprietary & ML20021A231 Non-Proprietary).

12. Regulatory Audit Plan for the HFC-FPGA Digital Platform Licensing Topical Report, April 27, 2020 (ADAMS Accession No. ML20043F266).
13. Regulatory Audit Report for the HFC-FPGA Digital Platform Licensing Topical Report, July 27, 2020 (ADAMS Accession No. ML20181A366).
14. Doosan HF Controls Corp, RAI Response for Amendment 4 to the HFC-6000 Safety Platform, June 25, 2020 (ADAMS Accession Nos. ML20195A834 Proprietary & ML20195A820 Non-Proprietary).
15. Submittal of Information for Amendment 4 to the HFC-6000 Safety Platform, August 29, 2017, including TR901-302-01 (ADAMS Package Accession No. ML18235A188).
16. HF Controls Corp., “HFC Controls Condition Report,” CR No: 2020-0093, May 14, 2020 (ADAMS Accession Nos. ML20307A673 Non-Proprietary).
17. HF Controls Corp., “HFC-6000 Control System VV0115 Isolation Test Summary Report,” TR-901-302-03, Revision A, October 26, 2020 (ADAMS Accession Nos. ML20307A671 Proprietary & ML20307A672 Non-Proprietary).